

STONE TOWN COUNCIL

Town Clerk

Les Trigg

Tel: 01785 619740

Fax: 01785 619741

15 Station Road

STONE

ST15 8JP

25 September, 2017

A meeting of the **GENERAL PURPOSES COMMITTEE** will be held in **St Michael's Suite at the Frank Jordan Centre, Lichfield Street, Stone**, on **TUESDAY 3 OCTOBER 2017 at 7:05pm**, or on the rising of the Council meeting if later.

I trust you will be able to attend.

Les Trigg
Town Clerk

AGENDA

1. **To receive apologies for absence**
2. **Declarations of Interest**
3. **Requests for Dispensations Received**
4. **To receive the report of the County Councillors**
 - County Councillor Mrs J Hood
 - County Councillor I Parry
5. **Representations from Members of the Public**

To consider representations from members of the public on items to be considered at this meeting, in accordance with the Council's scheme of public participation
6. **General Data Protection Regulation**

To receive the report of the Town Clerk (attached)
7. **Mayoral Allowances**

To receive the report of the Town Clerk (attached)

8. **Consultation on Stafford Borough Council's Planning Application Validation Criteria:**
To consider a consultation on Planning Application Validation Criteria.

Stafford Borough Council has refreshed its Planning Application Validation Criteria document with information guidance and support for those submitting planning applications. An eight-week consultation period will end on 3 November 2017.

Due to the size of the document this has been emailed to Members, but included in full on the Council's website. The Planning Validation Criteria and survey form can be found at:

<https://www.surveymonkey.co.uk/r/localvalidationcriteria>

9. **Civic Dinner**
To consider the change of date for the Civic Dinner in 2018 from Saturday 28 April to Saturday 21 April at the request of the Town Mayor.
10. **To consider the following request for a grant:**
- **AEDdonate** (supporting Coppice Estate to raise funds for a defibrillator)
11. **Purchase of Flags for Commemorative Events**
To consider the purchase of flags for commemorative events
12. **Craft Market**
To consider the impact on the Council's Craft Market of the proposed Stafford Maker's Market
13. **Non Cheque Payments**
To receive a list of non-cheque payments made by the Council during the period 1 July 2017 to 31 August 2017.
14. **Update from Working Groups:**
- a) Neighbourhood Plan Steering Group
 - b) To determine Protocol for Marking the Death of the Sovereign or other members of the Royal Family
15. **To receive reports from Town Councillors on attendance at meetings of local organisations and outside bodies as a representative of the Town Council**

Stone ATC – Mayor and Cllr M. Green

Age Concern Stone & District – Cllrs: Mrs K. Green and Mrs C. Collier

Stone Town Band – Mayor

Walton Community Centre – Cllr M. Green

Stafford & Stone Access Group – Cllr Mrs C. Collier

Stone Common Plot Trustees – Cllrs: M. Shaw, G. Collier, Mrs J. Hood and R. Kenney

Stone Community Hub Liaison Group – Cllrs: Mrs J. Farnham, M. Green, A. Osgathorpe, Mrs J. Hood and R. Kenney

SPCA Executive Committee – Cllr M. Williamson

Canal & River Trust – Canal Adoption Meeting – Cllrs: Mrs J. Hood, R. Kenney and P. Leason

16. **Exclusion of the Press and Public**

To resolve, pursuant to the Public Bodies (Admission to Meetings) Act 1960, that the Public and Press be excluded from the meeting whilst the next items of business are discussed on the grounds that publicity would be prejudicial to public interest by reason of the confidential nature of the debate

17. **Internal Audit**

To consider the report of the Town Clerk (attached)

Members of the public are welcome to attend the General Purposes Meeting as observers

Stone Town Council – General Purposes Committee

3rd October 2017

General Data Protection Regulations

Report of Town Clerk

Introduction

1. The purpose of this report is to consider changes to data protection requirements as a result of the General Data Protection Regulation (GDPR).

Background

1. Currently, data protection is controlled by the Data Protection Act 1998 (the 1998 Act). A new EU regulation known as the General Data Protection Regulation (GDPR) will come into force on 25th May 2018. The government has confirmed that the UK's decision to leave the EU will not affect this.
2. The main purposes of the GDPR are to increase the obligations of organisation when controlling personal data and to increase the rights of individuals to ensure that their personal data is respected and used only for legitimate purposes.
3. A copy of a GDPR overview document produced by the Information Commissioner and three briefings from the National Association of Local Councils (NALC) have been emailed to Councillors to provide additional information. These documents are also included with the version of this report on the Council's website.

Impact on the Council

4. The first direct impact on the Council will be the legal requirement to appoint a Data Protection Officer (DPO). The DPO could be an employee, or external to the organisation and appointed via a contract. The requirement for the DPO to have expert data protection knowledge and experience is likely to mean that virtually no town or parish council would be able to give the job to an existing employee. The time requirement for this role would, however, be relatively small for most local councils, so employing a new member of staff to undertake the role is unlikely to be viable for any but the largest town councils.
5. The Council is therefore likely to need to take on the services of an expert DPO via a contract, in a similar way to the Council's current contract for the provision of health and safety advice.
6. In my view, such a contract is likely to be best procured collaboratively by a group of Councils, and I have already had discussion with the Staffordshire Parish Councils Association (SPCA) to this effect. At present, however, there is no progress being made towards this.

7. Alternatives may be for one or more larger local councils to employ a member of staff, and provide the service at a cost to smaller parishes, or to purchase the service from a principal council such as Stafford Borough or the County Council, if they would be willing to offer such a service.
8. Clearly this is still a developing area, but there will undoubtedly be a cost to the Council of meeting this GDPR requirement. At present, I cannot even guess what that cost might be with any reliability, but would not be surprised if it ran to several thousand pounds per year.
9. Most of the other implications for the Council relate to the time required to review systems and process to ensure compliance with the new regulations, and the cost of any required changes to ensure that the provisions of the act can be met. Again, it is not possible at this stage to estimate this cost.
10. Attached as an appendix is a copy of the Information Commissioner's document "Preparing for GDPR – 12 Steps to Take Now" for the Committee's information.
11. Members should note that fines for breaching the regulations can very steep. Some breaches attract fines up to 20 million euros and others up to 10 million euros.

Conclusion

12. This report has set out the new legal requirements of the EU GDPR and outlined the potential impact on the Council.
13. Although costs cannot even be estimated with any accuracy at this stage, it is important that work commences on preparation without delay, or it may not be possible to meet the requirements of the GDPR in time for its implementation in May 2018. This could potentially open the Council up to large fines.
14. In particular, the Town Clerk will need the authority to pursue options for the provision of a Data Protection Officer (DPO) in time to ensure that the Council meets its obligations.

Recommendations

15. The Committee are recommended to:
 - a. Note the need for the Council to comply with the GDPR by the time it formally comes into force on 25th May 2018.
 - b. Authorise the Town Clerk to undertake the necessary preparation to meet the Council's obligations, including investigating options for the provision of a DPO.
 - c. Note that the Town Clerk will not incur any expenditure that cannot be met from existing budgets without seeking further approval from the Committee.

Reform of data protection legislation and introduction of the General Data Protection Regulation

Introduction

The Data Protection Act 1998 (“1998 Act”) is the main piece of legislation which governs the protection of personal data today. NALC’s guidance about the application of the 1998 Act to parish councils and, in Wales, to community councils is in Legal Topic Note 38 – Data Protection.

Legislative changes

Data protection law will significantly change on 25 May 2018, when the 2016 EU Directive known as General Data Protection Regulation (“GDPR”) takes effect. The GDPR will effectively replace the 1998 Act which implemented the EU Data Protection Directive (95/46/EC). The GDPR will be directly applicable in the UK without the need to implement national legislation. The Government has confirmed that the UK’s decision to leave the EU will not affect the commencement of the GDPR in 2018.

As with the 1998 Act, local authorities including parish councils and, in Wales, community councils will be subject to the GDPR. Many of the GDPR’s principles are the same as those in the 1998 Act. However GDPR imposes new obligations on data controllers and data processors and provides enhanced rights for individuals.

Preparing for the GDPR

Compliance with GDPR will have resource implications and we advise councils to start getting for ready for the introduction of GDPR without delay. We strongly recommend that councils follow the ICO’s easy to read guide entitled “Preparing for the General Data

Protection Regulation (GDPR) 12 steps to take now". This is available via the web link <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>.

The Information Commissioner's Office's ("ICO") website provides detailed guidance about GDPR which is available via the web link <https://ico.org.uk/for-organisations/data-protection-reform/>.

Data protection officer

As referenced in the above ICO guide, the GDPR will require some organisations such as public authorities to appoint a Data Protection Officer ("DPO"). The GDPR does not define the term "public authorities". However the term is expected to include local authorities. The DPO's responsibilities include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR.
- to monitor compliance with the GDPR including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits.
- to be the first point of contact for the regulator and for individuals whose data is processed

It is not yet known if the requirement for public authorities to appoint a DPO will extend to parish councils and, in Wales, to community councils. We will seek clarification from the Government and the ICO and provide another briefing when we have more information.

Reform of data protection legislation- General Data Protection Regulation and Data Protection Bill

General Data Protection Regulation

As explained in Legal Briefing L03-17, the EU regulation known as General Data Protection Regulation (“GDPR”) will come into force on 25 May 2018. As an EU regulation, the GDPR has direct effect; no national legislation is required for its provisions to apply. L03-17 confirmed that preparations for compliance with the requirements of GDPR will have significant resource implications for councils but should not be delayed. Compliance will be difficult if councils leave preparations until next year.

Getting ready for GDPR

1. With reference to L03-17 and the Information Commissioner Office’s (“ICO”) guide entitled “Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now” (available via the web link <https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>), the 12 steps required by councils include the following.
 - i) Ensuring that all councillors are aware that the law is changing and appreciate the impact this is likely to have. Councils should identify the activities/areas that could cause compliance problems under the GDPR.
 - ii) Auditing and documenting the personal data that they hold, where the personal data came from and how it is used or shared. This exercise will require resourcing.
 - iii) Identifying the lawful basis for processing and retaining personal data, documenting this and updating privacy notices. Under the Data Protection Act 1998 (“the 1998 Act”), a privacy notice is a reference to particular information which an organisation is required to provide to individuals when it is processing their personal data. This information includes confirmation of the identity of the organisation (i.e. the data controller) and, if any, the identity of the person processing personal data on behalf of the organisation (i.e. the data processor), the purpose(s) for which personal data will be processed and any other information which is necessary in the specific circumstances to enable the data processing to be fair. GDPR includes a longer and more detailed list of information that

must be provided in a privacy notice. GDPR also requires privacy notices to be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

Detailed advice about privacy notices is available from the ICO via <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/>. It includes guidance about how to write privacy notices. The ICO has also compiled examples of good and bad privacy notices which can be accessed via <https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf>

- iv) Reviewing how consents are sought, recorded, and managed. There is a fundamental difference between telling individuals how their personal data will be used and obtaining their consent for the same. Consents to a council must be freely given, specific, informed and unambiguous. There must be a positive opt-in consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and there must be simple ways for people to withdraw consent.
- v) Recruiting/procuring the services of a Data Protection Officer (“DPO”) who is required by GDPR to have expert knowledge of data protection law and practices. To clarify L03-17, GDPR requires “public authorities” (which includes local authorities such as parish councils and, in Wales, community councils) to appoint a DPO. More information about the DPO is in the Annex.

2. Councils may use the ICO’s self-assessment exercise in respect of compliance with GDPR. This is available via <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/>.
3. Councils should use the ICO’s website for detailed and practical guidance about GDPR via <https://ico.org.uk/for-organisations/data-protection-reform>.

Data Protection Bill

At the opening of Parliament on 21 June 2017, the Government committed itself to the introduction of the Data Protection Bill. Parts of the 1998 Act would need to be repealed for data processing to be within the scope of the GDPR and it is necessary to ensure that the 1998 Act does not duplicate or create inconsistencies with the GDPR, because the GDPR will be directly applicable.

In respect of the Data Protection Bill, the Government said its key priorities were:

- ensuring data protection rules were "suitable for the digital age";
- empowering individuals to have more control over their personal data;
- giving people the "right to be forgotten" when they no longer wanted an organisation to process their data - providing there were no legitimate grounds for an organisation retaining the data;
- modernising data processing procedures for law enforcement agencies;
- allowing police and the authorities to "continue to exchange information quickly and easily with international partners" to fight terrorism and other serious crimes;
- ensuring the country met its obligations while a member of the EU, and would help the UK maintain its "ability to share data with other EU members states and internationally after we leave the EU" and
- replacing the 1998 Act.

© NALC 2017

ANNEX

a) What are the DPO's responsibilities?

The DPO's minimum tasks are defined in Article 39 of GDPR. These are below.

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

The DPO will therefore have an "internal" and "external" aspect to their role, and it will be important that these do not interfere with one another.

The appointed DPO must at all times have regard to "the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing." This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the organisation's processing of personal data.

A DPO is not personally responsible in case of non-compliance with GDPR. Article 24 of GDPR makes it clear that data protection compliance is a responsibility of the data controller or the data processor.

b) Who may be appointed as the DPO?

Article 37(6) of the GDPR provides that the DPO may be an employee or external to the organisation, fulfilling the tasks on the basis of a service contract.

Where an employee is chosen as the DPO, there is nothing to prevent that individual from also performing other roles at the organisation, provided such roles do not affect his ability to adequately perform the role of DPO. The appointment of an internal DPO may also raise confidentiality and conflict of interest issues, and it will be important for organisations to develop policies and procedures to manage any such issues.

If the DPO is external, his function can be exercised based on a service contract with an individual or an organisation. Where an external DPO is selected, it will be

important for organisations to ensure that the DPO is able to form productive relationships with internal stakeholders and colleagues in order to perform the DPO role adequately.

c) Does the DPO need specific qualifications?

Article 37(5) of the GDPR provides that the DPO shall have expert knowledge of data protection law and practices. This should be proportionate to the type of processing that the organisation carries out, taking into consideration the level of protection the personal data requires. In the case of a public authority, the DPO should have sound knowledge of the organisation's administrative rules and procedures.

The DPO's relevant skills and expertise should ideally include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
- understanding of the processing operations carried out;
- understanding of information technologies and data security;
- knowledge of the business sector and the organisation and
- ability to promote a data protection culture within the organisation.

d) Resources for DPO

Article 38(2) of the GDPR provides that depending on the nature of the processing operations and the activities and size of the organisation, the following resources should be provided to the DPO:

- active support of the DPO's function by senior management ;
- sufficient time for DPOs to fulfil their tasks;
- adequate support in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate;
- official communication of the designation of the DPO to all staff;
- access to other services within the organisation so that DPOs can receive essential support, input or information from those other services and
- continuous training.

General Data Protection Regulation - summary of main provisions

Introduction

The EU regulation known as General Data Protection Regulation (“GDPR”) will come into force on 25 May 2018. The Government has also confirmed that it will introduce new legislation to repeal the Data Protection Act 1998 (“the 1998 Act”) and to ensure that new UK legislation does not create inconsistencies with the GDPR. It therefore seems likely that new UK legislation would be introduced before or on 25 May 2018.

Purpose of GDPR

GDPR contains terminology that councils will already be familiar with because they are included in the 1998 Act (see Legal Topic Note 38) e.g. personal data, data controller, data processor, data subject, subject access request, processing, and data protection principles.

GDPR builds on the legal framework established by the 1998 Act to balance the needs of organisations (businesses, not for profit and public bodies e.g. local authorities) in their capacities as data controllers and data processors to collect and use personal data against the rights of an individual to have his information (personal data) kept secure and private. GDPR has been introduced to address the privacy issues arising from a digital age in which personal data may be collected, transmitted, stored, manipulated and shared with relative ease e.g. using emails, websites, the internet and the cloud.

The purpose of the GDPR is to increase (i) the obligations on organisations when acting as data controllers and (ii) the rights of individuals to ensure that their personal data is respected and used only for legitimate purposes. It also imposes new obligations on data processors.

Put simply, personal data is data that relates to a living individual who can be recognised from that data. The categories of personal data processed by a council may include:

- communications with individual local residents including letters, complaints and council surveys;
- the council's employment and recruitment records (e.g. employment contracts, and job applications);
- contracts with individuals and contracts which require processing of personal data;
- arrangements with volunteers;
- communications with third parties e.g. principal authorities, CALCs, local charities, sports clubs, Disclosure and Barring Service ("DBS"), HMRC and staff pensions provider;
- the electoral roll and
- legal proceedings or transactions with individuals.

Summary of changes being introduced by GDPR

The annex to the Briefing provides a summary of the main provisions in the 1998 Act and the changes to be introduced by GDPR which are relevant to councils.



ANNEX

Subject	1998 Act requirements	GDPR requirements
Data protection principles	8 principles set out in Schedule 1.	<p>Same principles in 1998 Act but condensed to 6 principles listed below.</p> <p>Personal data must be:</p> <ul style="list-style-type: none">• Processed fairly, lawfully and in a transparent manner in relation to the data subject.• Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.• Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.• Accurate and, where necessary, kept up to date.• Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.• Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5).

Subject	1998 Act requirements	GDPR requirements
<p>Consent</p>	<p>Data Controllers are required to have valid purpose(s) for processing personal data and where the data controller is relying on an individual's consent, this is referenced in para 1 of schedule 2 (in respect of personal data) and in para 1 of schedule 3 (in respect of sensitive personal data- consent must be explicit).</p>	<p>Data controllers are required to have legitimate reason(s) for processing personal data and where the data controller is relying on an individual's consent, the data controller must be able to demonstrate that consent, by a statement or by a clear affirmative action, was freely given, specific, informed and unambiguous for each purpose that it being processed. Prior to giving consent, the individual shall be informed of his right to withdraw his consent at any time. In other words, it should be as easy to withdraw consent as to give it (Articles 4 and 7).</p>
<p>Consent for children</p>	<p>The 1998 Act does not specify an age at which a child will be considered able to give consent, and it is left to a data controller to decide, on a case by case basis, whether a child has the ability to understand the concept of their personal data and whether the consent given by the child is informed consent (i.e. is understood).</p>	<p>Limits the ability of a child under 16 to consent to their personal data being processed in respect of "information society services" e.g. online businesses or social networking sites. This means where personal data is being processed for a child under 16, consent must be obtained from the child's parent or custodian. An EU member state may lower the age that a child can give consent to processing of their data from 16 to 13. (Article 8). On 7 August 2017, the Government announced that it would use the Data Protection Bill to legislate that children aged 13 years or older can consent to their personal data being processed for information society services (see Legal Briefing L04-17 for more information about the Bill).</p>

Subject	1998 Act requirements	GDPR requirements
<p>Privacy notices (also known as fair processing notices)</p>	<p>Specifies basic information to be given by a data controller in a privacy notice (paras 1 – 5 of Part II of Schedule 1).</p>	<p>More information to be given by data controllers in privacy notices. This includes the following.</p> <ul style="list-style-type: none"> • the identity and the contact details of the data controller and, if any, of the controller's representative and of the data protection officer; • the purpose(s) of the processing; • the categories of personal data concerned; • the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations; • where possible, the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period; • the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; • the right to lodge a complaint with the ICO and • where the personal data is not collected from the data subject, any available information as to its source (Articles 13 and 14).



Legal Briefing

L05-17

August 2017

Subject	1998 Act requirements	GDPR requirements
Communications by data controllers		<p>There are new requirements on the data controller regarding the communications in a privacy notice and to the data subject relating to the rights of the data subject. Information provided must be a concise and intelligible form using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means (Article 12).</p>

Subject	1998 Act requirements	GDPR requirements
<p>Data controllers working with Data processors</p>	<p>Where personal data is processed by a data processor on behalf of a data controller, the data controller must (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and (b) take reasonable steps to ensure compliance with those measures.</p> <p>Where processing of personal data is carried out by a data processor on behalf of a data controller, the processing shall be carried out under a written contract under which (a) the data processor is to act only on instructions from the data controller, and (b) the data processor must comply with obligations equivalent to those imposed on a data controller by the seventh principle.</p> <p>(Paras 11 and 12 of Part II of Schedule 1)</p>	<p>The data controller is required to enter into a contract with the data processor which imposes the following obligations on the processor:</p> <ul style="list-style-type: none"> • Process the personal data only on the documented instructions of the controller. This is likely to mean that data processors cannot use cloud computing technology or services without the data controller's approval. • Comply with security obligations equivalent to those imposed on the controller under Article 32 of the GDPR. • Only employ staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality. • Enlist a sub-processor only with the prior permission of the controller. • Assist the controller in carrying out its obligations with regard to requests by data subjects to exercise their rights under Chapter III of the GDPR (including the right to transparency and information, the data subject access right, the right to rectification and erasure, the right to the restriction of processing, the right to data portability and the right to object to processing). • Assist the data controller in carrying out its data security obligations under Articles 32 to 36 of the GDPR (Article 28).

Subject	1998 Act requirements	GDPR requirements
<p>Privacy Impacts assessment (PIA)</p>	<p>A PIA is a process which helps an organisation to identify and reduce the privacy risks of new projects (e.g. use of CCTV or an IT system/ database for storing and accessing personal data) or policies. Conducting a PIA is not a requirement of the 1998 Act but it is regarded as good practice by the ICO. The ICO has issued a code of practice in respect of PIAs (s.51).</p>	<p>Where a type of processing in particular uses new technologies and the purpose(s) that the data controller wishes to process personal data poses high risks, it will have to carry out a data protection privacy impact assessment before such processing (Article 35). The ICO is expected to provide guidance about the type of processing that would demand a data protection privacy impact assessment.</p>
<p>Notification by data controllers</p>	<p>Notification to ICO to be included in register of data controllers (s.18).</p>	<p>The requirement to provide notification to ICO is replaced by a new requirement for data controllers to maintain a written record of processing activities under their responsibility. The written record shall include a description of the categories of data subjects and the categories of personal data, purpose(s) of processing, categories of recipients of personal data, time limits for erasure and description of technical and organisational measures to protect data. Data processors also have a new duty to maintain a written record of similar information. However, the obligation to maintain a written record does not apply to an organisation employing less than 250 persons unless the processing it carries out is likely to result in risks to the rights of data subjects, the processing is not occasional, or the processing includes special categories of data e.g. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, or processing criminal convictions and offences. (Article 30).</p>

Subject	1998 Act requirements	GDPR requirements
Appointment of Data Protection Officer (DPO)	No requirement.	Data controllers and data processors must designate a DPO in 3 situations which include where the processing is carried out by a public authority or body (e.g. local authorities including a parish council or, in Wales, a community council) (Article 37). More information about the DPO is in Legal Briefing L04-17 .
Notification to report personal data breaches	No requirement.	Data controllers are required to report to the ICO personal data breaches without delay and within 72 hours. A data processor must also notify a data controller without undue delay after becoming aware of a personal data breach (Article 33).
Fines	ICO may fine a data controller up to £500,000 for serious breaches (s.55A).	There are heavy fines for data controllers and data processors for a wide range of breaches. Some breaches (e.g. failing to comply with data subjects' rights or the principles for processing including conditions for consent) attract fines of up to 4% of annual turnover for the preceding year or 20 million Euros whichever is higher. For other breaches (e.g. failing to keep records of processing activities, to appoint a DPO or to comply with security obligations) the fine can be up to 2% of annual turnover or 10 million Euros, whichever is higher (Article 83).

Subject	1998 Act requirements	GDPR requirements
Individuals' rights	<p>Individuals have certain rights against data controllers</p> <ul style="list-style-type: none"> The right of access to personal data held by a data controller within 40 days of request upon payment of £10 fee (s.7). The right to prevent processing likely to cause damage or distress (s.10). The right to prevent processing for purpose of direct marketing (s.11). The right to object to decisions being taken by automated means (i.e. by a computer, by online profiling) (s.12). The right to claim compensation for damages caused by a breach of the 1998 Act (s.13). 	<p>Existing rights are strengthened and new rights are given. Individuals also have (limited) new rights against data processors.</p> <p>The right of access to personal data held by a data controller must be dealt with within one month of request and free of charge. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the data controller may charge a fee for providing the information or refuse to respond (Articles 12 & 15).</p> <p>The right to restriction of processing (Article 18).</p> <p>The right to object to the processing of personal data for direct marketing purposes (including profiling to the extent that it is related to direct marketing) (Article 21).</p> <p>The right not to be subject to automated decision-making (Article 22).</p> <p>The right to receive compensation from the data controller is retained and there is a new right to receive compensation from the data processor for the damage suffered as a result of an infringement of GDPR (Article 82).</p>

Subject	1998 Act requirements	GDPR requirements
Individuals' rights	<ul style="list-style-type: none"> The right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed (s.14). 	<p>The right to obtain from a data controller without undue delay the rectification of inaccurate personal data (Article 16).</p> <p>There is a new right to erase personal data (also known as the "right to be forgotten") which means that data subjects will be able to request that their personal data be erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with GDPR. However, the further retention of such data will be lawful in some cases e.g. amongst others, where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims. Where the data controller has made the personal data public and is obliged to erase the personal data it shall take reasonable steps to inform data controllers which are processing the personal data that the data subject has requested them to erase any links to, or copy or replication of that personal data (Article 17).</p>
<ul style="list-style-type: none"> None 	<ul style="list-style-type: none"> None 	<p>A new right to be notified by a data controller when a personal data breach is likely to result in a high risk to a data subject's rights (Article 34).</p>
<ul style="list-style-type: none"> None 		<p>A new right to data portability - to receive a copy of personal data or to transfer personal data to another data controller (Article 20).</p>



Legal Briefing

L05-17

August 2017

Further reading

The ICO's website has detailed guidance about:

- the new obligations for data controllers and data processors which can be accessed via <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/>

and

- the new rights for individuals which can be accessed via <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/>

Overview of the

General Data Protection

Regulation (GDPR)

Introduction	3
What's new	5
Principles	7
Key areas to consider	9
Individuals' rights	13
The right to be informed	14
The right of access	17
The right to rectification	19
The right to erasure	20
The right to restrict processing	22
The right to data portability	23
The right to object	25
Rights related to automated decision making and profiling	27
Accountability and governance	30
Breach notification	38
Transfer of data	40
National derogations	43

Introduction

Introduction

This overview highlights the key themes of the General Data Protection Regulation (GDPR) to help organisations understand the new legal framework in the EU. It explains the similarities with the existing UK Data Protection Act 1998 (DPA), and describes some of the new and different requirements. It is for those who have day-to-day responsibility for data protection.

This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The ICO is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. We acknowledge that there may still be questions about how the GDPR would apply in the UK on leaving the EU, but this should not distract from the important task of compliance with the GDPR.

With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to individuals. The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will work with government to stay at the centre of these conversations about the long term future of UK data protection law and to provide our advice and counsel where appropriate.

Who does the GDPR apply to?

- The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the DPA – ie the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the [Law Enforcement](#)

[Directive](#), processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Further reading in the GDPR

[See Articles 3, 28-31 and Recitals 22-25, 81-82](#)

External link

What information does the GDPR apply to?

Personal data

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9). These categories are broadly the same as those in the DPA, but there are some minor changes.

For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

Further reading in the GDPR

[See Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51](#)

External link

What's new

What's new

We will update this page monthly to highlight and link to what's new in our Overview of the GDPR.

June 2017

The Article 29 Working Party's consultation on their [guidelines on high risk processing and data protection impact assessments](#) closed on 23 May. We await the adoption of the final version.

May 2017

We have updated our [GDPR 12 steps to take now document](#)

We have added a [Getting ready for GDPR checklist to our self-assessment toolkit](#)

April 2017

We have published our [profiling discussion paper for feedback](#).

March 2017

We have published our [draft consent guidance for public consultation](#).

January 2017

Article 29 have published the following guidance, which is now included in our overview:

- [Data portability](#)
- [Lead supervisory authorities](#)
- [Data protection officers](#)

Next steps

Article 29 are planning the following guidance:

- Consent
- Transparency
- Profiling
- High risk processing
- Certification
- Administrative fines
- Breach notification
- Data transfers

The ICO are planning guidance on:

- Contracts and liability

Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

The principles are similar to those in the DPA, with added detail at certain points and a new **accountability** requirement. The GDPR does not have principles relating to individuals' rights or overseas transfers of personal data - these are specifically addressed in separate articles (see GDPR Chapter III and Chapter V respectively).

The most significant addition is the accountability principle. The GDPR requires you to show **how** you comply with the principles – for example by documenting the decisions you take about a processing activity. [This is explained in greater detail later in this guide.](#)

Article 5 of the GDPR requires that personal data shall be:



- (a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

Further reading in the GDPR

[See Article 5 and Recital 39](#)

Key areas to consider

Lawful processing

For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing” under the DPA.

It is important that you determine your lawful basis for processing personal data and document this.

This becomes more of an issue under the GDPR because your lawful basis for processing has an effect on individuals’ rights. For example, if you rely on someone’s consent to process their data, they will generally have stronger rights, for example to have their data deleted.

The GDPR allows member states to introduce more specific provisions in relation to Articles 6(1)(c) and (e):



“(c) processing is necessary for compliance with a legal obligation”;

“(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”

These provisions are particularly relevant to public authorities and highly regulated sectors.

The tables below set out the lawful bases available for processing personal data and special categories of data.

Lawfulness of processing conditions

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.

Conditions for special categories of data

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

Further reading in the GDPR

 [See Articles 6-10 and Recitals 38, 40-50, 59](#) 

External link

Consent



Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent. Public authorities and employers will need to take particular care to ensure that consent is freely given.

Consent has to be verifiable, and individuals generally have more rights where you rely on consent to process their data.

Remember that you can rely on other lawful bases apart from consent – for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

Further reading in the GDPR

 [See Articles 4\(11\), 6\(1\)\(a\), 7, 8, 9\(2\)\(a\) and Recitals 32, 38, 40, 42, 43, 51, 59, 171](#) 
External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidelines on consent in 2017.

Next steps for the ICO

We have published our [draft consent guidance for public consultation](#). The deadline for responses has now passed. We will analyse the feedback received and feed this into the final version which is due for publication in the summer.

Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data.

Privacy notices for children

Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand.

Online services offered to children

If you offer an 'information society service' (ie online service) to children, you may need to obtain consent from a parent or guardian to process the child's data.

The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding

'parental responsibility' – but note that it does permit member states to provide for a lower age in law, as long as it is not below 13.

'Information society services' includes most internet services provided at the user's request, normally for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

Further reading in the GDPR

 [See Article 8 and Recital 38, 58, 71](#) 

External link

Next steps for the ICO

The ICO is working on the issue of children's personal data and we aim to publish output from this in 2017.

Individuals' rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This part of the overview explains these rights.

The right to be informed

In brief...

The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

In more detail...

What information must be supplied?

The GDPR sets out the information that you should supply and when individuals should be informed.








The information you supply is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this.

Much of the information you should supply is consistent with your current obligations under the DPA, but there is some further information you are explicitly required to provide.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The table below summarises the information you should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer		
Purpose of the processing and the lawful basis for the processing		
The legitimate interests of the controller or third party, where applicable		
Categories of personal data		

Any recipient or categories of recipients of the personal data		
Details of transfers to third country and safeguards		
Retention period or criteria used to determine the retention period		
The existence of each of data subject's rights		
The right to withdraw consent at any time, where relevant		
The right to lodge a complaint with a supervisory authority		
The source the personal data originates from and whether it came from publicly accessible sources		
Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data		
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.		



When should information be provided?	At the time the data are obtained.	<p>Within a reasonable period of having obtained the data (within one month)</p> <p>If the data are used to communicate with the individual, at the latest, when the first communication takes place; or</p> <p>If disclosure to another recipient is envisaged, at the latest, before the data are</p>
---	------------------------------------	---

disclosed.

Further reading – ICO guidance

 [Privacy notices, transparency and control](#)
For organisations

Further reading in the GDPR

 [See Articles 12\(1\), 12\(5\), 12\(7\), 13 and 14 and Recitals 58-62](#) 
External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidance on transparency in 2017

The right of access

In brief...

What information is an individual entitled to under the GDPR?

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

These are similar to existing subject access rights under the DPA.

In more detail...

What is the purpose of the right of access under GDPR?

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Can I charge a fee for dealing with a subject access request?

You must provide a copy of the information free of charge. The removal of the £10 subject access fee is a significant change from the existing rules under the DPA.

However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee must be based on the administrative cost of providing the information.

How long do I have to comply?

You will have less time to comply with a subject access request under the GDPR. Information must be provided without delay and at the latest within one month of receipt.

You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

What if the request is manifestly unfounded or excessive?

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

How should the information be provided?

You must verify the identity of the person making the request, using “reasonable means”.

If the request is made electronically, you should provide the information in a commonly used electronic format.

The GDPR introduces a new best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well.

The right to obtain a copy of information or to access personal data through a remotely accessed secure system should not adversely affect the rights and freedoms of others.

What about requests for large amounts of personal data?

Where you process a large quantity of information about an individual, the GDPR permits you to ask the individual to specify the information the request relates to (Recital 63).

The GDPR does not introduce an exemption for requests that relate to large amounts of data, but you may be able to consider whether the request is manifestly unfounded or excessive.

Further reading in the GDPR

 [See Article 12, 15 and Recital 63](#) 

External link

The right to rectification

In brief

When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

In more detail...

How long do I have to comply with a request for rectification?

You must respond within one month.

This can be extended by two months where the request for rectification is complex.

Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Further reading in the GDPR

 [See Articles 12, 16 and 19](#) 

External link

The right to erasure

In brief...

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

In more detail...

When does the right to erasure apply?

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

There are some specific circumstances where the right to erasure does not apply and you can refuse to deal with a request.

When can I refuse to comply with a request for erasure?

You can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes;
or
- the exercise or defence of legal claims.

How does the right to erasure apply to children’s personal data?

There are extra requirements when the request for erasure relates to children’s personal data, reflecting the GDPR emphasis on the enhanced protection of such information, especially in online environments.

If you process the personal data of children, you should pay special attention to existing situations where a child has given consent to processing and they later request erasure of the data (regardless of age at the time of the request), especially on social networking sites and internet forums. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent (Recital 65).

Do I have to tell other organisations about the erasure of personal data?

If you have disclosed the personal data in question to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

While this might be challenging, if you process personal information online, for example on social networks, forums or websites, you must endeavour to comply with these requirements.

As in the example below, there may be instances where organisations that process the personal data may not be required to comply with this provision because an exemption applies.

Example

A search engine notifies a media publisher that it is delisting search results linking to a news report as a result of a request for erasure from an individual. If the publication of the article is protected by the freedom of expression exemption, then the publisher is not required to erase the article.

Further reading in the GDPR

 [See Articles 17, 19 and Recitals 65 and 66](#) 

External link

The right to restrict processing

In brief...

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

In more detail...

When does the right to restrict processing apply?

You will be required to restrict the processing of personal data in the following circumstances:



- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.

If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

You must inform individuals when you decide to lift a restriction on processing.

Further reading in the GDPR

 [See Articles 18, 19 and Recital 67](#) 

External link

The right to data portability

In brief...

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

Example

midata is used to improve transparency across the banking industry by providing personal current account customers access to their transactional data for their account(s), which they can upload to a third party price comparison website to compare and identify best value. A price comparison website displays alternative current account providers based on their own calculations.

In more detail...

When does the right to data portability apply?

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

How do I comply?

You must provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information must be provided free of charge.

If the individual requests it, you may be required to transmit the data directly to another organisation if this is technically feasible. However, you are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual.

How long do I have to comply?

You must respond without undue delay, and within one month.

This can be extended by two months where the request is complex or you receive a number of requests. You must inform the individual within one month of the receipt of the request and explain why the extension is necessary.



Where you are not taking action in response to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Further reading in the GDPR

 [See Articles 12, 20 and Recital 68](#) 

External link

Further reading from the Article 29 Working Party

The Article 29 Working Party has published [guidelines](#)  and [FAQs](#)  on data portability for organisations.

The right to object

In brief...

When does the right to object apply?

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

In more detail...

How do I comply with the right to object?

If you process personal data for the performance of a legal task or your organisation's legitimate interests

Individuals must have an objection on "grounds relating to his or her particular situation".

You must stop processing the personal data unless:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

If you process personal data for direct marketing purposes

You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.

You must deal with an objection to processing for direct marketing at any time and free of charge.

You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

These requirements are similar to existing rules under the DPA.

If you process personal data for research purposes

Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes.

If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

If your processing activities fall into any of the above categories and are carried out online:

You must offer a way for individuals to object online.

Further reading in the GDPR

 [See Articles 12, 21 and Recitals 69 and 70](#) 

External link

Rights related to automated decision making and profiling

In brief...

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

In more detail...

When does the right apply?

Individuals have the right *not to be subject to a decision* when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

You must ensure that individuals are able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

Does the right apply to all automated decisions?

No. The right does not apply if the decision:

- is necessary for entering into or performance of a contract between you and the individual;
- is authorised by law (eg for the purposes of fraud or tax evasion prevention); or
- based on explicit consent. (Article 9(2)).

Furthermore, the right does not apply when a decision does not have a legal or similarly significant effect on someone.

What else does the GDPR say about profiling?

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work;
- economic situation;
- health;

- personal preferences;
- reliability;
- behaviour;
- location; or
- movements.

When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place.

You must:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences.
- Use appropriate mathematical or statistical procedures for the profiling.
- Implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions taken for the purposes listed in Article 9(2) **must not**:

- concern a child; or
- be based on the processing of special categories of data unless:
 - you have the explicit consent of the individual; or
 - the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.

Further reading in the GDPR


 [See Articles 4\(4\), 9, 22 and Recitals 71, 72](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidelines on profiling in 2017.

Next steps for the ICO

We have published our [profiling discussion paper for feedback](#) . The deadline for responses has now passed. We will analyse the feedback received and will publish a summary of responses

in due course. This feedback will inform our input into the drafting of the EU guidance on profiling and automated decision-making.

Accountability and governance

In brief...

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

In more detail...

- [What is the accountability principle?](#)
- [Records of processing activities \(documentation\)](#)
- [Data protection by design and by default](#)
- [Data protection impact assessments](#)
- [When does a Data Protection Officer need to be appointed under the GDPR?](#)
- [Codes of conduct and certification mechanisms](#)

What is the accountability principle?

The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

How can I demonstrate that I comply?

You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
 - Data minimisation;

- Pseudonymisation;
 - Transparency;
 - Allowing individuals to monitor processing; and
 - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

You can also:

- Adhere to approved codes of conduct and/or certification schemes. See the [section on codes of conduct and certification](#) for more detail.

Records of processing activities (documentation)

As well as your obligation to provide comprehensive, clear and transparent privacy policies (see section on [Individual rights](#)), if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

- processing personal data that could result in a risk to the rights and freedoms of individual; or
- processing of special categories of data or criminal convictions and offences.

What do I need to record?

You must maintain internal records of processing activities. You must record the following information. There are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

Further reading in the GDPR

 [See Article 30, Recital 82.](#) 

External link

Further reading from the Article 29 Working Party

The Article 29 Working Party has published [guidelines](#) and [FAQs](#) on lead supervisory authorities. These are intended to assist in identifying which is the lead supervisory authority when a controller or processor is carrying out cross-border processing of personal data.

Data protection by design and by default

Under the GDPR, you have a general obligation to implement technical and organisational measures to show that you have considered and integrated data protection into your processing activities.

Under the DPA, privacy by design has always been an implicit requirement of the principles - eg relevance and non-excessiveness - that the ICO has consistently championed. The ICO has published [guidance in this area](#).

Further reading in the GDPR

 [See Article 25 and Recital 78](#)

External link

Data protection impact assessments

What is a data protection impact assessment?

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

While not a legal requirement under the DPA, the ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach. See the ICO's [Conducting privacy impact assessments code of practice](#) for good practice advice.

When do I need to conduct a DPIA?

You must carry out a DPIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal

effects – or similarly significant effects – on individuals.

- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity.

- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?


- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Further reading in the GDPR

 [See Articles 35, 36 and 83 and Recitals 84, 89-96](#) 

External link

Next steps

The Article 29 Working Party has [published guidelines on high risk processing and DPIAs](#) . They invited comments on these and this consultation has now closed.

When does a Data Protection Officer need to be appointed under the GDPR?

Under the GDPR, you **must** appoint a data protection officer (DPO) if you:

- are a public authority (except for courts acting in their judicial capacity);
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking);
or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations

under the GDPR.

What are the tasks of the DPO?

The DPO's minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

What does the GDPR say about employer duties?

You must ensure that:

- The DPO reports to the highest management level of your organisation – ie board level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

Can we allocate the role of DPO to an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests.

You can also contract out the role of DPO externally.

Does the data protection officer need specific qualifications?

The GDPR does not specify the precise credentials a data protection officer is expected to have.

It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Further reading in the GDPR

 [See Articles 37-39, 83 and Recital 97](#) 

External link

Further reading from the Article 29 Working Party

The Article 29 Working Party has published [guidelines](#) and [FAQs](#) on DPOs.

Further reading from the ICO

We are currently considering whether the ICO can provide any further detail over and above the Article 29 Working Party guidelines. We will add any additional advice we are able to provide here in due course.

Codes of conduct and certification mechanisms

The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply.

The specific needs of micro, small and medium sized enterprises must be taken into account.

Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers your processing activity becomes available, you may wish to consider working towards it as a way of demonstrating that you comply.

Adhering to codes of conduct and certification schemes brings a number of benefits over and above demonstrating that you comply. It can:

- improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data.
- provide mitigation against enforcement action; and
- improve standards by establishing best practice.

When contracting work to third parties, including processors, you may wish to consider whether they have signed up to codes of conduct or certification mechanisms.

Who is responsible for drawing up codes of conduct?

Governments and regulators can **encourage** the drawing up of codes of conduct.

Codes of conduct may be created by trade associations or representative bodies.

Codes should be prepared in consultation with relevant stakeholders, including individuals (Recital 99).

Codes must be approved by the relevant supervisory authority; and where the processing is cross-border, the European Data Protection Board (the EDPB).

Existing codes can be amended or extended to comply with the requirements under the GDPR.

What will codes of conduct address?

Codes of conduct should help you comply with the law, and may cover topics such as:

- fair and transparent processing;
- legitimate interests pursued by controllers in specific contexts;
- the collection of personal data;
- the pseudonymisation of personal data;
- the information provided to individuals and the exercise of individuals' rights;
- the information provided to and the protection of children (including mechanisms for obtaining parental consent);
- technical and organisational measures, including data protection by design and by default and security measures;
- breach notification;
- data transfers outside the EU; or
- dispute resolution procedures.

Practical implications

If you sign up to a code of conduct, you will be subject to mandatory monitoring by a body accredited by the supervisory authority.

If you infringe the requirements of the code of practice, you may be suspended or excluded and the supervisory authority will be informed. You also risk being subject to a fine of up to 10 million Euros or 2 per cent of your global turnover.

Adherence to a code of conduct may serve as a mitigating factor when a supervisory authority is considering enforcement action via an administrative fine.

Who is responsible for certification mechanisms?

Member states, supervisory authorities, the EDPB or the Commission are required to encourage the establishment of certification mechanisms to enhance transparency and compliance with the Regulation.

Certification will be issued by supervisory authorities or accredited certification bodies.

What is the purpose of a certification mechanism?

A certification mechanism is a way of you demonstrating that you comply, in particular, showing that you are implementing technical and organisational measures.

A certification mechanism may also be established to demonstrate the existence of appropriate safeguards related to the adequacy of data transfers.

They are intended to allow individuals to quickly assess the level of data protection of a particular product or service.

Practical implications

Certification does not reduce your data protection responsibilities.

You must provide all the necessary information and access to your processing activities to the certification body to enable it to conduct the certification procedure.

Any certification will be valid for a maximum of three years. It can be withdrawn if you no longer meet the requirements of the certification, and the supervisory authority will be notified.

If you fail to adhere to the standards of the certification scheme, you risk being subject to an administrative fine of up to 10 million Euros or 2 per cent of your global turnover.

Further reading in the GDPR

 [See Articles 40-43, 83 and Recitals 98, 99,100, 148, 150, 151](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will produce guidelines on certification in 2017. It also intends to publish guidelines, which are already under development, on imposing administrative fines.

Breach notification

In brief...

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

In more detail...

What is a personal data breach?

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Example

A hospital could be responsible for a personal data breach if a patient's health record is inappropriately accessed due to a lack of appropriate internal controls.

What breaches do I need to notify the relevant supervisory authority about?

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

When do individuals have to be notified?

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

What information must a breach notification contain?

- The nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned; and

- the categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

How do I notify a breach?

A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.

If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

What should I do to prepare for breach reporting?

You should make sure that your staff understands what constitutes a data breach, and that this is more than a loss of personal data.

You should ensure that you have an internal breach reporting procedure in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.

In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Further reading in the GDPR

 [See Articles 33, 34, 83 and Recitals 85, 87, 88](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will produce guidelines on the notification of personal data breaches in 2017.

Transfer of data

In brief...

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

In more detail...

When can personal data be transferred outside the European Union?

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Transfers on the basis of a Commission decision

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

Further reading in the GDPR

 [See Article 45 and Recitals 103-107 & 169](#) 

External link

Transfers subject to appropriate safeguards

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted in to administrative arrangements between public authorities or bodies authorised

by the competent supervisory authority.

Further reading in the GDPR

 [See Article 46 and Recitals 108-10 & 114](#) 

External link

Next steps for the Article 29 Working Party

According to its workplan, the Article 29 Working Party will publish guidelines on data transfers based on binding corporate rules and contractual clauses in 2017.

The GDPR limits your ability to transfer personal data outside the EU where this is based only on your own assessment of the adequacy of the protection afforded to the personal data.

Authorisations of transfers made by Member States or supervisory authorities and decisions of the Commission regarding adequate safeguards made under the Directive will remain valid/remain in force until amended, replaced or repealed.

Further reading in the GDPR

 [See Article 83 and 84 and Recitals 148-152](#) 

External link

The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

The first three derogations are not available for the activities of public authorities in the exercise of their public powers.

Further reading in the GDPR

 [See Article 49 and Recitals 111 & 112](#) 

External link

What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?

Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

However, such transfers are permitted only where the transfer:

- is not being made by a public authority in the exercise of its public powers;
- is not repetitive (similar transfers are not made on a regular basis);
- involves data related to only a limited number of individuals;
- is necessary for the purposes of the compelling legitimate interests of the organisation (provided such interests are not overridden by the interests of the individual); and
- is made subject to suitable safeguards put in place by the organisation (in the light of an assessment of all the circumstances surrounding the transfer) to protect the personal data.

In these cases, organisations are obliged to inform the relevant supervisory authority of the transfer and provide additional information to individuals.

Further reading in the GDPR

 [See Article 49 and Recital 113](#) 

External link

National derogations

What derogations does the GDPR permit?

Article 23 enables Member States to introduce derogations to the GDPR in certain situations. These are similar to the existing exemptions from rights and duties in the DPA.

Member States can introduce exemptions from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

Other Member State derogations or exemptions

Chapter IX provides that Member States can provide exemptions, derogations, conditions or rules in relation to specific processing activities. These include processing that relates to:

- freedom of expression and freedom of information;
- public access to official documents;
- national identification numbers;
- processing of employee data;
- processing for archiving purposes and for scientific or historical research and statistical purposes;
- secrecy obligations; and
- churches and religious associations.

Further reading in the GDPR

 [See Articles 6\(2\), 6\(3\), 9\(2\)\(a\), 23 and 85-91 and Recitals 71, 50, 53, 153-165](#) 

External link

Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

Preparing for the General Data Protection

Regulation (GDPR) 12 steps to take now



1

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2

Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5

Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6

Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7

Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8

Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10

Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11

Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12

International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

Introduction

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist you, as well as contributing to guidance that the Article 29 Working Party is producing at the European level. These are all available via the ICO's [Overview of the General Data Protection Regulation](#). The ICO is also working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about implementation in your sector.

It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Some parts of the GDPR will have more of an impact on some organisations than on others (for example, the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

1

Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

2

Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3

Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to

complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

The ICO's [Privacy notices code of practice](#) reflects the new requirements of the GDPR.

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the

information free of charge.

5

Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

6

Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to

help you comply with the GDPR's 'accountability' requirements.

7

Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

You should read the [detailed guidance](#) the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

8

Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9

Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10

Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should also familiarise yourself now with the [guidance the ICO has produced on PIAs](#) as well as [guidance from the Article 29 Working Party](#), and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

11

Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has [produced guidance for organisations on the designation, position and tasks of DPOs](#).

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

12

International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

The Article 29 Working party has produced [guidance on identifying a controller or processor's lead supervisory authority](#).

Stone Town Council – General Purposes Committee

3rd October 2017

Mayoral Allowances

Report of Town Clerk

Introduction

1. The purpose of this report is to consider Mayoral allowances for the 2018-19 and subsequent municipal years.

Background

1. Currently the Council pays an allowance of £2,319.15 to the Town Mayor and £637.57 to the Deputy Mayor. These amounts are paid in full as single lump sums, shortly after they take up office.
2. These are the only payments made to the Mayor and Deputy in order to carry out their official duties. Having received these allowances, they are expected to meet the full costs of transport, tickets for events, appropriate clothing and any other related expenditure themselves. There is no requirement for the Mayor or Deputy to account to the Council for their spending. The Council therefore has no records to show how the money has been used, though it is likely that the allowances fall well short of the full costs of undertaking these roles.
3. Since the commencement of the current municipal year, clarification has been received regarding the payment of these allowances which means that the Council will need to change some of its practices for future years. Details are set out below.

Mayor's Allowance

4. The current practice of paying a lump sum allowance direct to the Mayor, with the Mayor then being responsible for declaring their own income tax cannot continue. Any lump sum payment must now be paid through the PAYE system to deduct income tax at source. The Council, however, has some options:

- a. **Continue with current lump sum payment system, but deduct tax via PAYE.**

The Mayor should be able to claim this tax back by demonstrating to HM Revenue and Customs (HMRC) that the allowance represented "reasonable reimbursement of the expenses of an unpaid office" and that the expenses were incurred "wholly, exclusively and necessary in performance of their duties". This would, however, be each Mayor's personal responsibility, not the Council's.

If this option is adopted, it would also be sensible to change the current system of paying a single lump sum for the year to paying monthly, otherwise National Insurance payments would also need to be deducted.

- b. **Pay a smaller lump sum allowance but meet some Mayoral costs by direct payment from the Council.**

The Council could pay direct for event tickets, and reimburse the Mayor for travel either by public transport, where a receipt can be produced, or by private car based on a mileage claim. The residual allowance would provide recompense for items such as appropriate clothing, small tokens such as flowers, donations to charities and the purchase of raffle tickets at events.

This would reduce the income tax initially paid by the Mayor and the amount that the Mayor would need to justify to HMRC in order to reclaim tax paid.

- c. **Pay no lump sum allowance, and meet Mayoral costs by reimbursement only.**

This would remove any need to deal with taxation, but it would not be legally possible to reimburse any items considered to be optional, or not exclusively for mayoral use. Such items could include, for example, clothing, donations and drinks at events.

Deputy Mayor's Allowance

- 5. Following clarification, the Council can no longer pay a lump sum allowance to the Deputy Mayor.
- 6. The Council could pay direct for event tickets, and reimburse the Deputy Mayor for travel either by public transport, where a receipt can be produced, or by private car based on a mileage claim. It could also reimburse other expenses provided that they were not optional, and were exclusively for use when deputising for the Mayor.
- 7. This is effectively the same as Mayoral option c above.

Conclusion

- 8. This report has set out the current position with regard to the payment of allowances and expenses to the Mayor and Deputy Mayor of the Council. It clarifies that the Council can no longer pay Mayoral allowances without the deduction of income tax, and that a lump sum allowance can no longer be paid to the Deputy Mayor.
- 9. The Committee is asked to consider how it wishes to reimburse Mayoral expenses in the future.

Recommendation

- 10. That the Committee considers the options available and determines a future policy for the reimbursement of Mayoral expenses.



**Stafford Borough Council
Development Management**

**Planning Application
Validation Guidance and Local
Validation Criteria**

August 2017

To be used for all applications except Discharge of
Conditions and Lawful Development Certificates.

A quick guide for Householders is included in the Annex Contents

Information	Page Number
Introduction	4
Pre application discussions	5
How to use the Validation Criteria	5
Photographs	5
Making an Application Valid	6
Guidance for Outline Applications	6
National Requirements	
Application Forms	7
Design and Access Statement	7
Fee	8
Location plan	8
Site Plan	9
Block Plan	9-10
Existing and Proposed Elevations	10
Existing and Proposed Floor Plans	10-11
Existing and Proposed Site Sections and Finished Floor and Site Levels	11-12
Roof Plan	12
Agricultural Holdings Certificate	12
Ownership Certificate	13
Notice	13
Local Requirements	
1) Affordable Housing Statement	14
2) Agricultural Need Statement	14-15
3) Air Quality Assessment	15
4) Biodiversity Survey and Report	16-17
5) Cannock Chase Special Area of Conservation (SAC)	17
6) Coal Mining Risk Assessment	18-19
7) Economic Statement	19
8) Environmental Statement / EIA	19-20
9) Flood Risk Assessment (FRA)	20-21

**Stafford Borough Council Planning Application Validation Criteria
August 2017**

10) Foul Sewerage Assessment	21-22
11) Heritage Asset Statement	23-24
12) Land Contamination Assessment	24
13) Landscape Visual Impact Assessment	25
14) Landscaping Details	25
15) Lighting Assessment	26
16) Masterplan	26
17) Noise and Vibration Assessments	26
18) Open Space Assessment	27
19) Parking and Access Arrangements	28
20) Planning Obligations (Section 106 Agreements) / Unilateral Undertakings / Draft Heads of Terms	29
21) Retention of Local Community Facility or Service Statement	30
22) Statement of Community Involvement	31
23) Structural Survey	31
24) Telecommunications Development – Supplementary Information	32
25) Town Centre Use / Retail Impact Assessments	32-33
26) Transport Assessment / Transport Statement	33-34
27) Travel Plan	35
28) Tree Survey / Assessment	35-36
29) Ventilation / Extraction Statement	36-37
30) Viability Assessment	37
31) Water Quality Statement	37-38
Annex Items	
Householder Checklist	39-41

Stafford Borough Council Planning Application Validation Criteria August 2017

Introduction

Before we can make an assessment on your planning application, you need to provide us with forms, plans and other information. The information that you need to provide depend on the type of application that you're making. These Validation Criteria explain the information that we need for all applications (known as the National Validation Requirements) and the information that we ask for at Stafford Borough Council (known as the Local Validation Requirements). Where we ask for additional information, we will only do so if we really need it. The amount of information that we normally need depends on the scale of the proposal. Once we have all of the information, your application can be registered as valid and we can start the assessment process.

The Plan for Stafford Borough sets out the policy context for the local validation criteria.

Legislation

The following pieces of legislation are used to validate applications:

- The Town and Country Planning Act 1990 (as amended by the Planning and Compulsory Purchase Act 2004)
- The Town and Country Planning (Development Management Procedure) (England) Order 2015 (DMPO)

The Regulation that we work to, when asking for further information is:

- Regulation 4 of the Town and Country Planning (Applications) Regulations 1988. This enables a Local Planning Authority to direct applicant's to supply any further information, plans and drawings that are necessary to make a decision. Applications for Outline permission are slightly different – for more information see page 6.

This includes providing any reasonable evidence to answer any queries.

If you are not happy with the information that we are asking for, you can challenge the request (details of how to do this are set out in DMPO).

Policy

Each piece of information that we ask for is linked to a piece of national or local policy. This explains why we are asking for that particular detail.

Stafford Borough Council Planning Application Validation Criteria August 2017

Pre-application Discussions

The National Planning Policy Framework (NPPF) that was introduced in March 2012 says that we have a key role to play in encouraging applicants (or their agents) to take maximum advantage of the pre-application stage of the planning process.

If we can identify any potential issues with your application before it is made, this helps to avoid delays in making a decision.

If you are thinking about making a planning application and would like some advice before you apply, please contact Planning Support on 01785 619 327.

How to use the Validation Criteria

If you are making a Householder application, which is for things like an extension or conservatory, our quick guide for Householders can be found in **the ANNEX**.

For other applications, you will need to make sure that you provide all of the information in the National Requirements (see pages 7-12). You then need to look through the Local Requirements to identify the additional information needed. The requirements are listed alphabetically, but the column headed 'Types of application that require this information' will tell you whether your application type is included.

For all types of information (plans, forms and all other documents), unless you are making your application electronically, we need three copies of everything to be provided.

Photographs

Whilst we no longer require photographs and a plan showing where the photographs were taken from and their direction, providing photos helps us to spot anything on site that you might need to supply more information on.

Stafford Borough Council Planning Application Validation Criteria August 2017

Making an Application Valid

If the information listed for your application type is not provided then we won't be able to make your application valid and start work on our assessment. If we receive your application and some information is missing, we will contact you.

Where an application is submitted, its receipt will be acknowledged in writing. However, if we consider that the application is invalid, we will let the applicant know what extra information we need.

Please note that if plans are not consistent with each other, and we cannot reasonably assess the proposal that is being made, we won't be able to validate the application.

Guidance for Outline Applications

Applications for outline planning permission generally don't need to include details of any proposed 'reserved matters' unless the matters include layout, scale or access.

If we receive an application for outline planning permission, but decide that the application should not be considered separately from all or any of the reserved matters, we must notify the applicant within one month from the receipt of the application that further details are needed.

Information must include:

- Use – the use or uses proposed for the development and any distinct development zones within the site identified.
- The amount of development proposed for each use (for retail this should be the gross retail floorspace expressed as square metres).
- Indicative access points

In addition, major applications for outline permission should also include a Design and Access Statement.

Stafford Borough Council Planning Application Validation Criteria August 2017

National Requirements

Application Forms

All planning applications need to be made using a standard application form. Each application type has its own standard form, which can be found on our web-site (which links to the Planning Portal, the Government website for Planning).

How many copies are needed?

Applications can either be submitted electronically through the Planning Portal or in paper copies. Please bear in mind that if a paper application is completed, you will need to provide 3 copies before your application can be made valid.

Design and Access Statement

A Design and Access Statement must accompany Listed Building applications, applications for one or more dwellings or building(s) with a floor space of 100m² or more in a Conservation Area and major applications, for example 10 houses or more, floorspace 1,000m² or site area of 1 hectare or more, for both outline and full planning permission.

A Design and Access Statement is a concise report supporting a planning application that should explain and justify the proposal in a structured way. The Design and Access Statement should cover both the design principles and concepts that have been applied to the proposed development, and how issues related to access to the development have been dealt with.

For Listed Buildings, the statement should address:

- the special architectural and historic interest of the building
- the particular physical features of the building that justify its designation as a Listed Building; and
- the building's setting.

The legislative requirements are set out in Regulation 3A of the Planning (Listed Buildings and Conservation Areas) Regulations 1990.

Stafford Borough Council Planning Application Validation Criteria August 2017

Fee

An application cannot be made valid without the correct fee.

Fees are set nationally and vary depending on the type and size of the application. The full list of charges can be found on our website.

Please note, if your application is approved and conditions are included that we need to discharge, there will be a further fee.

Location Plan

All applications must include a location plan based on an up to date map.

What scale should the plan be drawn to?

Either 1:1250 or 1:2500. Very occasionally we might need a different scale plan but we will let you know if this is the case.

What should the plan show?

Wherever possible at least two named roads and the surrounding buildings. The buildings should be numbered or named so that the exact location of the application site is clear.

The application site should be edged clearly with a red line. It should include all land necessary to carry out the proposed development – for example, land required for access to the site from a public highway, visibility splays, landscaping, car parking and open areas around buildings. The red edge is required to be drawn to the nearest adopted highway as per the below guidance.

<https://www.gov.uk/guidance/making-an-application>

A blue line should be drawn around any other land owned by the applicant, close to or adjoining the application site.

If the location plan that you provide uses an Ordnance Survey map base, the plan must include your Ordnance Survey copyright licence.

Stafford Borough Council Planning Application Validation Criteria August 2017

How many copies are needed?

One copy for applications made electronically through the Planning Portal, or 3 copies for paper applications.

Site Plan

What scale should the plans be drawn to?

The site plan should be drawn at a scale of 1:500 or 1:200

What should the plan show?

- The direction of north
- The proposed development in relation to the site boundaries and other existing buildings on the site, with written dimensions including those to the boundaries
- All buildings, roads and footpaths on land adjoining the site, including access arrangements
- All public rights of way crossing or adjoining the site (including footpaths, bridleways, restricted byway or byway open to all traffic)
- The position of all trees on the site, and those on adjacent land that could influence or be affected by the development
- The extent and type of any hard surfacing
- Details of boundary treatments (walls, fences, railings, hedges, landscaping) and where this is proposed and existing

How many copies are needed?

One copy for applications made electronically through the Planning Portal, or 3 copies for paper applications.

Block Plan

A block plan is a larger scale version of the location plan, showing the same application boundary with a greater level of information.

What scale should the plans be drawn to?

The scale should be 1:100 or 1:200 and they should show the site boundaries.

Stafford Borough Council Planning Application Validation Criteria August 2017

What should the plan show?

- Site boundaries
- The type and height of boundary treatment (walls, fences, hedges)
- The position of any building or structure on the other side of the boundaries

How many copies are needed?

One copy for applications made electronically through the Planning Portal, or 3 copies for paper applications.

Existing and Proposed Elevations

What scale should the plans be drawn to?

The scale should be 1:50 or 1:100

What should the plans show?

- They should clearly show the proposed works in relation to what is already there.
- All sides of the proposal must be shown and these should indicate, where possible, the proposed building materials and the style, materials and finish of windows and doors. Blank elevations must also be included.
- Where a proposed elevation adjoins another building or is in close proximity, the drawings should clearly show the relationship between the buildings, and detail the positions of the openings on each property.

How many copies are needed?

One copy for applications made electronically through the Planning Portal, or 3 copies for paper applications.

Existing and Proposed Floor Plans

What scale should the plans be drawn to?

The scale should be 1:50 or 1:100

Stafford Borough Council Planning Application Validation Criteria August 2017

What should the plans show?

- They should explain the proposal in detail.
- Where existing buildings or walls are to be demolished these should be clearly shown. The drawings submitted should show details of the existing building(s) as well as those for the proposed development. New buildings should also be shown in context with adjacent buildings (including property numbers or names where applicable).

How many copies are needed?

One copy for applications made electronically through the Planning Portal, or 3 copies for paper applications.

Existing and Proposed Site Sections, and Finished Floor and Site Levels

What scale should the plans be drawn to?

The scale should be 1:50 or 1:100

What should the plans show?

- They should show a cross section(s) through the proposed building(s)
- In all cases where a proposal involves a change in ground levels, illustrative drawings should be submitted to show both existing and finished levels, to include details of foundations and eaves, and how encroachment onto adjoining land is to be avoided
- Full information should also be submitted to demonstrate how proposed buildings relate to existing site levels and neighbouring development. The plans should show existing site levels and finished floor levels (with levels related to a fixed offsite datum point) and also show the proposals in relation to adjoining buildings. This will be required for all applications involving new buildings
- Levels should also be taken into account in the formulation of design and access statements

Stafford Borough Council Planning Application Validation Criteria August 2017

For householder development, the levels may be clear from floor plans and elevations, but particularly in the case of sloping sites, you will need to show how proposals relate to existing ground levels or where ground levels outside the extension would be modified.

How many copies are needed?

One copy for applications made electronically through the Planning Portal, or 3 copies for paper applications.

Roof Plan

A roof plan is used to show the shape of the proposed roof.

What scale should the plans be drawn to?

Usually roof plans are drawn at a scale smaller than the scale used for the floor plans.

What should the plans show?

- Roofing materials
- Vents and their location

How many copies are needed?

One copy for applications made electronically through the Planning Portal, or 3 copies for paper applications.

Agricultural Holdings Certificate

This certificate is required whether or not the site includes an agricultural holding. It is included in the standard application form.

All agricultural tenants must be notified prior to the submission of the application.

This certificate is not required if the applicant is making an application for reserved matters, renewal of temporary planning permission, discharge or variation of conditions, works to trees covered by Tree Preservation Orders, or express consent to display an advertisement.

**Stafford Borough Council Planning Application Validation Criteria
August 2017**

Ownership Certificates

All applications for planning permission, except for approval of reserved matters, must include the appropriate certificate of ownership. An ownership certificate A, B, C or D must be completed stating the ownership of the property. The certificates are included in the standard application forms.

For this purpose an 'owner' is anyone with a freehold interest, or leasehold interest, the unexpired term of which is not less than 7 years.

Notice

Where an application is for land that is not wholly owned by the applicant, it will be necessary to complete Certificate B (or on occasion Certificate C or D) and serve Notice 1 on owners of the application site.

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
1	Affordable Housing Statement	<p>National Planning Policy Framework paragraphs 47, 50, 54, 89, 159, 173,174, 177</p> <p>Circular 6/1998 Planning and Affordable Housing</p> <p>Plan for Stafford Borough: Policy C2</p>	<p>When 12 or more dwellings are proposed at Stafford, Stone, Eccleshall, Gnosall Woodseaves, Barlaston, Tittensor, Yarnfield, Hixon, Great Haywood, Little Haywood/Colwich, Haughton & Weston.</p> <p>When 10 or more dwellings are proposed across all other areas of the Borough</p>	<p>New residential development of 12 or more dwellings at Stone, Eccleshall, Gnosall Woodseaves, Barlaston, Tittensor, Yarnfield to provide 40% affordable dwellings.</p> <p>New residential development of 12 or more dwellings at Stafford, Hixon, Great Haywood, Little Haywood/Colwich, Haughton & Weston to provide 30% affordable dwellings.</p> <p>New residential development of 10 or more dwellings across all other areas of the Borough to provide 30% affordable housing. .</p> <p>An independent economic viability assessment must be provided if a lower figure is being proposed as part of a new development.</p> <p>Further Advice</p> <p>Stafford Borough Council Health and Housing Group: 01785 619 000</p> <p>Stafford Borough Forward Plans Team: 01785 619000</p>
2	Agricultural Need Statement	<p>National Planning Policy Framework paragraphs 28, 55, 112, 120</p> <p>Plan for Stafford Borough: Policy E2</p>	New agricultural buildings and agricultural workers dwellings	<p>The statement must include:</p> <ul style="list-style-type: none"> • The size of the agricultural holding • Details of any additional rented land and duration of the rental agreement • Details of any other buildings used on the land, including floorspace and current use • Details of what the building will be used for, including floorspace

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
2	Agricultural Need Statement (Continued)			<ul style="list-style-type: none"> • Number of animals kept (where relevant) • Number of employees and their hours worked <p>Further Advice</p> <p>Stafford Borough Council Development Management: 01785 619 337</p>
3	Air Quality Assessment	<p>National Planning Policy Framework paragraph 124</p> <p>Plan for Stafford Borough: Policy N5</p>	<p>In, or adjacent to an Air Quality Management Area, all applications for new housing development, industrial, commercial and leisure development</p> <p>Where the development could itself result in the designation of an Air Quality Management Area</p> <p>Where the grant of planning permission would conflict with, or render unworkable, elements of a local authority's Air Quality Action Plan</p> <p>Within 50m of the edge of M6 carriageway</p>	<p>Applications must be supported by information that enables full consideration of the impact of the proposal on the air quality of the area</p> <p>Where Air Quality Management Areas cover regeneration areas, developers should provide an Air Quality Assessment as part of their planning application.</p> <p>Further Advice</p> <p>Stafford Borough Council Pollution Control Officer: 01785 619 402</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
4	Biodiversity Survey and Report	<p>National Planning Policy Framework paragraphs 118-119, 192</p> <p>Plan for Stafford Borough: Policy N1, N4, N5 Wildlife and Countryside Act 1981</p> <p>Conservation of Habitats and Species Regulations 2012</p> <p>Protection of Badgers Act 1992</p>	<p>Where a proposed development may have possible impacts on wildlife and biodiversity</p> <p>Renewals of existing consents should include an update on any information provided with the original application</p>	<p>Information must be provided on existing biodiversity interests and possible impacts on them.</p> <p>Where proposals are being made for mitigation and/or compensation measures, information to support those proposals will also be needed.</p> <p>Where appropriate, accompanying plans should indicate any significant wildlife habitats or features, and the location of any habitats of any species protected under the Wildlife and Countryside Act 1981, the Conservation of Habitats and Species</p> <p>Applications for development in the countryside that will affect areas designated for their biodiversity interests are likely to need to include assessments of the impacts and proposal for long term maintenance and management. This information might form part of an Environmental Statement, where one is necessary.</p> <p>Certain proposals which include work such as the demolition of older buildings or roof spaces, removal of trees, scrub, hedgerows or alterations to water courses may affect protected species and will need to provide information on them, any potential impacts for them and any mitigation proposals for such impacts.</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
4	Biodiversity Survey and Report (continued)			<p>Advice should include a requirement for a Staffordshire Ecological Records search of the application site and a 500 metre buffer, and presentation of this information. This will help planning officers to assess whether a sufficient biodiversity survey and assessment has been carried out.</p> <p>Further Advice Stafford Borough Council Biodiversity Officer 01785 619 676</p> <p>Natural England Standing Advice www.naturalengland.org.uk/</p>
5	Cannock Chase Special Area of Conservation (SAC) Statement	<p>National Planning Policy Framework paragraph 115, 118-119</p> <p>Plan for Stafford Borough Council: Policy N6</p> <p>ODPM Circular 06/2005</p>	Applications for residential development within 8km of Cannock Chase Special Area of Conservation	<p>The Council has sufficient evidence to demonstrate that an increase of 1 net dwelling or more within the 8km zone will have an impact on the Cannock Chase Special Area of Conservation.</p> <p>For the Council to carry out their Duty of Care as a competent authority in respect of the European Habitats Directive applicants / agents must mitigate against this impact in some way. This may include a financial contribution to improve nearby areas of open space or more significant mitigation schemes, or for larger sites on-site open space may be factored into the scheme.</p> <p>A statement detailing an appropriate mitigation scheme must be submitted with any application proposing an increase in dwellings within the 8km zone around Cannock Chase SAC.</p> <p>Further Advice Stafford Borough Council Forward Planning: 01785 619 000</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
6	Coal Mining Risk Assessment (CMRA)	National Planning Policy Framework paragraph 120-121, 144	All non-householder applications for operational development that fall within the Coal Mining Development Referral Areas as defined by the Coal Authority and held by Stafford Borough Council	<p>The Coal Mining Risk Assessment must be prepared by a suitably qualified and competent person. It should:</p> <p>Include site specific coal mining information (including past / present / future underground mining, shallow coal workings, mine entries (shafts or adits), mine gas, within an area which has a current licence to extract coal, geological features, any recorded surface hazards, or within a former or present surface mining (old opencast) area)</p> <p>Identify what risks these coal mining issues, including cumulative effects, pose to the proposed development</p> <p>Identify how coal mining issues have influenced the proposed development, and whether any other mitigation measures are required to manage those issues and / or whether any changes have been incorporated into the development</p> <p>Any development that involves intrusive activities which intersect, disturb or enter any coal seams, coal mine workings or mine entries will require the prior written permission of The Coal Authority.</p> <p>Please note - if an Environmental Statement is required by the Town and Country Planning (Environmental Impact Assessment) Regulations 2011 as amended, it is suggested that the CMRA is included within the Environmental Statement.</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
6	Coal Mining Risk Assessment (CMRA) (continued)			<p>Further Advice</p> <p>The Coal Authority website: www.coal.gov.uk/services/planning The Coal Authority Planning and Local Authority Liaison Department : 01623 637 119 or planningconsultation@coal.gov.uk</p>
7	Economic Statement	<p>National Planning Policy Framework paragraphs 7, 8, 17-22, 26, 28</p> <p>Plan for Stafford Borough: Policy E1, E2, E3, E6, E7</p>	All major applications that include a commercial element	<p>A supporting statement of any regeneration and economic benefits and costs from the proposed development.</p> <p>The statement must include:</p> <p>Details of new jobs provided or supported Relative floor space totals for each proposed use (where known) Any community benefits Reference to any regeneration strategies that might lie behind or be supported by the proposal</p> <p>Further Advice</p> <p>Stafford Borough Council Economic Development Manager: 01785 619 748</p>
8	Environmental Statement (Environmental Impact Assessment – EIA)	<p>National Planning Policy Framework paragraph 192</p> <p>The Town and Country Planning (Environmental Impact Assessment)</p>	Where an Environmental Impact Assessment is needed Schedule 4 sets out the information required in an Environmental Statement	<p>The information in the Environmental Statement has to be taken into consideration when the Local Planning Authority decides whether to grant planning consent. It may be helpful for a developer to request a “screening opinion” (to determine whether an EIA is required) from the Local Planning Authority before submitting a planning application.</p> <p>In cases where a full EIA is not required, the Local Planning</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
8	Environmental Statement (Environmental Impact Assessment – EIA) (Continued)	Regulations 2017		<p>Authority may still require environmental information to be provided.</p> <p>An applicant may request a scoping opinion (to determine the issues that need to be addressed in an EIA) before submitting the application. In addition, pre-application discussions will assist in identifying the issues that need to be addressed in an EIA.</p> <p>Further Advice</p> <p>Stafford Borough Council Development Management: 01785 619 337</p>
9	Flood Risk Assessment (FRA)	<p>National Planning Policy Framework paragraphs 99-104, 192</p> <p>Technical Guidance to the National Planning Policy Framework (CLG 3/12)</p> <p>Plan for Stafford Borough: Policy N1, N2</p>	<p>In Floodzone 1 any development site of 1 hectare or above</p> <p>In Floodzones 2 and 3 all developments</p> <p>Any development other than minor development in a designated critical drainage area which has been notified to the Local Planning Authority by the Environment Agency (Rising Brook).</p>	<p>The Flood Risk Assessment must:</p> <ul style="list-style-type: none"> • identify and assess the risks of all forms of flooding to and from the development, and demonstrate how these flood risks will be managed, taking climate change into account • identify opportunities to reduce the probability and consequences of flooding • include the design of surface water management systems including Sustainable Drainage Systems (SUDs), and address the requirement for safe access to and from the development in areas at risk from flooding • be prepared by the developer in consultation with the Local Planning Authority with reference to their published new Local Plan documents and any Strategic Flood Risk Assessment • form part of an Environmental Statement when one is required by the Town and Country Planning

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
9	Flood Risk Assessment (FRA) (continued)			<ul style="list-style-type: none"> • (Environmental Impact Assessment) Regulations 2011 as amended <p>In preparing a Flood Risk Assessment the developer will be required to demonstrate that a sequential approach to site selection has been undertaken, and that there are no other more suitable sites available.</p> <p>For Householder development a simplified procedure is available in the Environment Agency Standing Advice http://www.environment-agency.gov.uk/research/planning/82584.aspx</p> <p>Further Advice</p> <p>Environment Agency http://www.environment-agency.gov.uk/homeandleisure/floods/default.aspx</p> <p>Further information on SUDs is available at https://www.staffordshire.gov.uk/environment/Flood-Risk-Management/Information-for-Planners-and-Developers.aspx</p>
10	Foul Sewerage Assessment	Water Industries Act 1999 National Planning Policy Framework paragraphs	Where an application proposes a new building to connect to the existing drainage system Developments involving the	A foul drainage assessment must include: <ul style="list-style-type: none"> • a full assessment of the site • site location • suitability for storing, transporting and treating sewage.

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
		120-121 Plan for Stafford Borough: Policy N2	disposal of trade waste or foul sewage effluent	Where connection to the mains sewer is not practical, then the foul / non-mains drainage assessment must demonstrate: <ul style="list-style-type: none"> • why the development cannot connect to the public mains sewer system and • show the alternative means of disposal are satisfactory.
10	Foul Sewerage Assessment (Continued)			<p>Guidance on what should be included in a non-mains drainage assessment is given in the NPPG and Building Regulations Approved Document Part H and in BS6297.</p> <p>If the proposed development results in any changes / replacement to the existing system or the creation of a new system, scale plans of the new foul drainage arrangements should also be provided.</p> <p>This will include:</p> <ul style="list-style-type: none"> • a location plan • cross sections / elevations • system specification <p>If connection to any of the above requires crossing land that is not in the applicant's ownership, other than within a public highway, then notice will need to be served on the owners of that land.</p> <p>Details may also be needed of surface water run-off limitation.</p> <p>It is possible that the right to connect storm waters to foul sewers in areas where there are no storm drains may be withdrawn by</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
				<p>amendment to section 106 of the Water Industry Act 1991.</p> <p>Further Advice</p> <p>Severn Trent: www.stwater.co.uk Environment Agency</p>
11	Heritage Asset Statement	<p>National Planning Policy Framework paragraphs 128-141</p> <p>Plan for Stafford Borough: Policy N8, N9</p>	<p>Any application affecting a heritage asset or its setting</p> <p>Heritage Assets include:</p> <ul style="list-style-type: none"> • Listed Buildings • Conservation Areas • Scheduled Monuments • Archaeological sites • Registered parks and gardens <p>Applications involving the disturbance of ground within a known area of archaeological significance</p> <p>Major applications or significant infrastructure works where archaeological remains may survive</p> <p>Hedgerow removal may need</p>	<p>The statement must include:</p> <ul style="list-style-type: none"> • A description of the significance of the heritage assets affected, and the contribution of their setting to that significance • The level of detail should be proportionate to the importance of the heritage asset and no more than is sufficient to understand the potential impact of the proposal on the significance of the heritage asset • The relevant historic environment record should have been consulted • The heritage assets themselves should have been assessed using appropriate expertise, where necessary, given the application's impact • Where an application site includes, or is considered to have the potential to include, heritage assets with archaeological interest, Local Planning Authorities should require developers to submit an appropriate desk-based assessment and, where desk-based research is insufficient to properly assess the interest, a field evaluation • An assessment of the impact of the proposal should be set out in the application (within the design and access statement when this is required) as part of the explanation of the design concept. It should detail the sources that

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
			a Heritage Statement where it forms part of a significant historic landscape or an area of archaeological potential	<p>have been considered and the expertise that has been consulted</p> <p>Stafford Borough Council will not validate applications where the extent of the impact of the proposal on the significance of any heritage assets affected cannot adequately be understood from</p>
11	Heritage Assess Statement (continued)			<p>the application and supporting documents.</p> <p>Further Advice</p> <p>Stafford Borough Council Conservation Officer: 01785 619 337 Staffordshire County Council: 0300 111 8000 (Staffordshire County Archivist , Staffordshire County Archaeologist)</p>
12	Land Contamination Assessment	<p>National Planning Policy Framework paragraphs 120-122</p> <p>Plan for Stafford Borough: Policy N2</p>	All applications (excluding Householders) where new development is proposed on land that is, or may have been, affected by contamination	<p>The assessment must include:</p> <ul style="list-style-type: none"> • An extended assessment of contamination in line with National Planning Policy Framework: Section 11 • Enough information to determine the existence or otherwise of contamination, its nature and the risks it may pose, and whether these can be satisfactorily reduced to an acceptable level <p>Where contamination is known or suspected, or the proposed use would be particularly vulnerable for example residential use, the applicant should provide such information with the application as is necessary to determine whether the proposed development can</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
				<p>proceed.</p> <p>Further Advice</p> <p>Stafford Borough Council Pollution Control Officer: 01785 619 402 Environment Agency www.environment-agency.gov.uk</p>
13	Landscape Visual Impact Assessment	Plan for Stafford Borough: Policy N8	Polytunnels; wind turbines	An assessment in accordance with current best practice and guidance, in particular GLVIA3 published by the Landscape Institute and the Institute of Environmental Management and Assessment.
14	Landscaping Details	<p>National Planning Policy Framework paragraphs 58-59</p> <p>Plan for Stafford Borough: Policy N1</p>	All major applications	<p>A landscaping scheme should:</p> <ul style="list-style-type: none"> • Be drawn to scale (usually 1:100 or 1:200) • Show full details of proposed landscaping • Include details of proposed species, height at planting, spacing and densities • Include measures for the ongoing protection and maintenance of landscaping <p>For sites that are considered to be particularly sensitive, in landscape or visual terms, a Landscape and Visual Impact Assessment (LVIA) should be undertaken.</p> <p>Further Advice</p> <p>Guidelines for LVIA 3rd Edition 2013 published by the Landscape Institute and the Institute of Environmental Management and Assessment.</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
				Stafford Borough Council Development Management: 01785 619 337
15	Lighting Assessment	Plan for Stafford Borough: Policy N1	All commercial and leisure applications proposing external illuminations	<p>The assessment must include:</p> <ul style="list-style-type: none"> • A layout plan with beam orientation and light spillage • A schedule of the equipment used in the design • The hours of use (when the lighting will be switched on) • Details of future maintenance <p>Further Advice Publication: Lighting in the countryside: Towards good practice (1997)</p>
16	Masterplan	Plan for Stafford Borough: Policy Stafford 2, Stafford 3, Stafford 4, Stone 2	Residential development within Strategic Development Locations	A comprehensive land use masterplan in accordance with Policy Stafford 2, Stafford 3, Stafford 4 and Stone 2
17	Noise and Vibration Assessments	<p>Noise Policy Statement for England March 2010</p> <p>National Planning Policy Framework paragraph 123</p> <p>Plan for Stafford Borough: Policy N1</p>	<p>All applications likely to have an impact on existing noise or vibration sensitive developments</p> <p>All applications that introduce or expose noise or vibrations into an area where it would have an adverse impact</p>	<p>Applicants are advised to seek specialist expertise and to discuss their proposals in the first instance with Stafford Borough Council's Environmental and Health Service to find out whether a Noise and Vibration Assessment is needed. Where an assessment is needed it must:</p> <ul style="list-style-type: none"> • Consider the advice, recommendations or requirements contained in British Standards BS6472: 2008 <i>Guide to Evaluation of Human Exposure to Vibration in Buildings</i> Part 1 and Part 2 and BS7385-2: 1993 <i>Evaluation and Measurement for Vibration in Buildings</i> Part 1

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
		Environmental Protection Act 1990 Clean Neighbourhoods Act 2005 Licencing Act 2003 Noise Act 1996		<p>Further Advice Stafford Borough Council Environmental and Health Service: 01785 619 402 World Health Organisation Guidelines for Community Noise World Health Organisation Night Noise Guidelines for Europe British Standards: BS4142, BS8233, BS7445</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
18	Open Space Assessment	<p>National Planning Policy Framework paragraphs 73, 74, 77</p> <p>National Planning Policy Guidance</p> <p>Plan for Stafford Borough: Policy C7</p>	Residential applications of 11 dwellings or more to provide an on-site or off-site contribution to open space, sport and recreation facilities in accordance with the Local Standards (Appendix G of The Plan for Stafford Borough)	<p><u>Developments Within Open Spaces</u></p> <p>Applications must include:</p> <ul style="list-style-type: none"> • Plans showing any areas of existing or proposed open space within or adjoining the application site • <p><u>On-site or off-site Provision</u></p> <p>Where open space and/or associated facilities are proposed to be provided on-site or off-site the application must define them and provide a statement that includes:</p> <ul style="list-style-type: none"> • Maintenance specification for the works • How the facility will be initially installed and maintained to that specification for at least 10 years <p><u>Financial Contributions</u></p> <ul style="list-style-type: none"> • Where open space cannot be entirely provided on site, a financial contribution will be required through a Planning Obligation (Section 106 Agreement) <p>Further Advice</p> <p>Stafford Borough Council Parks and Open Spaces Development Officer: 01785 619 514</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
19	Parking and Access Arrangements	<p>National Planning Policy Framework paragraphs 32, 35, 39, 40</p> <p>Plan for Stafford Borough: Policy T2 and Appendix B: Car Parking Standards</p>	All applications, including householders, that involve new, or changes to existing, parking and access arrangements	<p>The site layout plan must include;</p> <ul style="list-style-type: none"> • Details of existing parking provision and access • Details of proposed parking provision and access • Details of the level of provision (including cycles) <p>Details about any access works should include:</p> <ul style="list-style-type: none"> • Information about how that supports the design • Include micro-modelling analysis and a Stage 2 Safety Audit where access is served via a traffic signalled junction, roundabout or priority junction, with right turn facility <p>For access only, simple priority junctions or dropped crossings, details must include:</p> <ul style="list-style-type: none"> • Details of existing and proposed visibility splays • Details of speed surveys where relaxation to normal visibility requirements are being sought <p>Further Advice Staffordshire County Council Roads and Highways Standing Advice: 0300 111 8000 highways@staffordshire.gov.uk</p> <p>Manual for Streets 2</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
20	Planning Obligations / Unilateral Undertakings (Section 106 Agreements) / Draft Heads of Terms	Circular 05/2005: Planning Obligations National Planning Policy Framework paragraph 173-177, 203-206 Plan for Stafford Borough: Policies C2, C7, I1	All major applications unless trigger points are not hit. See 'What information is required' column for trigger points Other developments where the Section 106 agreement can make an otherwise unacceptable proposal acceptable in planning terms	<p>The application must include either:</p> <ul style="list-style-type: none"> A draft Planning Obligation (Section 106) obligation based on Stafford Borough Council's standard template or A statement of the proposed Heads of Terms, a location plan and Land Registry details, solicitor details and confirmation that Stafford Borough Council's legal fees will be met <p>Further Advice Stafford Borough Council Legal Services: 01785 619 220</p> <p><u>Trigger Points:</u></p> <p>Affordable Housing = When 12 or more dwellings are proposed at Stafford, Stone, Eccleshall, Gnosall, Woodseaves, Barlaston, Tittensor, Yarnfield, Hixon, Great Haywood, Little Haywood/Colwich, Haughton & Weston.</p> <p>Affordable Housing = When 3 or more dwellings are proposed across all other areas of the Borough</p> <p>Housing development will be required to provide contributions for new infrastructure, either on site or off site, as set out in the Infrastructure Delivery Plan, including for open space, sport and recreation in line with the Local Space Standards (Appendix G of The Plan for Stafford Borough)</p> <p>For the Education trigger points at primary and secondary school levels please contact Staffordshire County Council Education and Learning: 0300 111 8000</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
21	Retention of Local Community Facility or Service Statement	National Planning Policy Framework paragraph 28 Plan for Stafford Borough: Spatial Principle 7 and Policy E8	Applications for redevelopment or change of use of any premises outside Stafford or Stone currently used, or last used to provide essential facilities or services which support the local community	<p>A statement must be provided that addresses the following:</p> <ul style="list-style-type: none"> • a viability test that the use concerned is no longer economically viable, that all reasonable efforts have been made to sell or let the property in its current use at a realistic price for a period of at least 12 months, the use cannot be provided by some other means or is genuinely redundant • the premises or site, or an unused part of the building, cannot be readily used for or converted to another community facility • the facility / service which will be lost will be adequately supplied or met by an easily accessible existing or new facility in the local area or the settlement concerned, unless it has been accepted as redundant under (a) above • the facility was not required to be provided and / or retained as part of a planning permission, or as a new development <p>Further Advice</p> <p>Stafford Borough Council Development Management: 01785 619 000</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
22	Statement of Community Involvement	National Planning Policy Framework paragraphs 188-189 Stafford Borough Statement of Community Involvement	All major applications	<p>The statement must:</p> <ul style="list-style-type: none"> • Set out how the applicant has undertaken pre-application consultation with the community • Demonstrate that the views of the local community have been sought and taken into account in the formulation of development proposals <p>Further Advice</p> <p>Stafford Borough Council Development Management: 01785 619 337</p>
23	Structural Survey	National Planning Policy Framework paragraphs 28, 55, 120-130, 133, 136, 141 The Plan for Stafford Borough: Policy E2	<p>All barn conversion proposals, except where the barn has already been fully converted</p> <p>Applications involving the demolition of a building or structure, Listed Building or Listed structure or unlisted building in a Conservation Area</p>	<p>Structural surveys must be carried out by qualified structural surveyors, and detail:</p> <ul style="list-style-type: none"> • The existing structural condition of the building • Any recommended remedial works to improve its condition, if possible • For barn conversions, the survey must also include: • Whether the existing building is capable of conversion without significant rebuilding • The nature, type and amount of work required to allow the proposed use to take place <p>Further Advice</p> <p>Stafford Borough Council Development Management/Conservation Officer: 01785 619 337</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
24	Telecomms Development - Supplementary Information	Code of Practice on Mobile Network Development (2013) National Planning Policy Framework paragraphs 45-46 Plan for Stafford Borough: Policy E1	Telecommunications applications	Applications must include the following: <ul style="list-style-type: none"> • The area of the search • Details of any consultation carried out • Details of the proposed structure • The technical justification and information about the proposed development • A signed declaration that the equipment and installation has been designed in full compliance of the radio frequency exposure guidelines of the International Commission of Non-Ionizing Radiation Protection (ICNIRP) <p>Further Advice Code of Practice on Mobile Network Development (2002)</p>
25	Town Centre Use / Retail Impact Assessments	National Planning Policy Framework paragraphs 23-27 Plan for Stafford Borough: Policy E8	Applications for main town centre uses that are not in an existing town centre and are not in accordance with the Plan for Stafford Borough must include a Sequential Assessment Applications for retail, office and leisure developments at Stafford over 1,000m ² gross floorspace, developments at Stone over 500m ² gross floorspace and developments	Retail Impact Assessments for town centre uses in an edge or out-of-centre location as part of development proposals greater than 1000 m ² gross floorspace at Stafford, greater than 500 m ² gross floorspace at Stone and greater than 300m ² gross floorspace at local centres must assess: <ul style="list-style-type: none"> • The impact on existing investment within centres • The impact on the vitality and viability of town centres • The impact of the proposal on in-centre trade / turnover and trade in the wider area • The current and future consumer expenditure capacity in the catchment area • Whether the proposal is of an appropriate scale and what impact it may have on locally important impacts <p>Further Advice Stafford Borough Council Forward Planning: 01785 619 000</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
25	Town Centre Use / Retail Impact Assessments (continued)		<p>at local centres over 300 m² and not in accordance with the Plan for Stafford Borough.</p> <p>Applications in an existing town centre not in accordance with the Plan for Stafford Borough which would substantially increase the attraction of the centre to an extent that the development could impact on other centres.</p>	
26	Transport Assessment / Transport Statement	<p>Circular 02/2007: Planning and the Strategic Road Network</p> <p>National Planning Policy Framework paragraph 32</p> <p>Plan for Stafford Borough: Policy T1</p>	All applications likely to generate significant traffic movements	<p>For a definition of significant transport implications see https://www.staffordshire.gov.uk/transport/staffshighways/highwayscontrol/Documents/GuidelinesforTransportAssessmentsandTravelPlansJan.pdf</p> <p>Where an assessment is considered to be necessary, these should be submitted and considered by Staffordshire County Council Highways Authority prior to the registration of the Planning Application.</p> <p>When Planning Applications require an assessment, the application will be required to submit a 'Transport Assessment Validation Form' signed by the applicant and a representative of Staffordshire County</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
26	Transport Assessment / Transport Statement (Continued)			<p>a) A Transport Assessment (TA) or Transport Statement</p> <p>b) (TS) is required, and that the assessment accompanying the Planning Application, including its conclusions, have been agreed with Staffordshire County Council Highways Authority</p> <p>c) A TA or TS is required, and that the assessment accompanying the Planning Application, including its conclusions, have been discussed but the Applicant and Staffordshire County Council Highways Authority are in dispute</p> <p>d) An assessment is not required</p> <p>Further Advice</p> <p>Department for Transport: https://www.gov.uk/government/organisations/department-for-transport Manual for Streets 2 (March 2007) Circular 02/2007: Planning and the Strategic Road Network Council Highway Authority indicating that: A draft Travel Plan must:</p> <ul style="list-style-type: none"> • Outline how the transport implications of the development are going to be managed to ensure minimal environmental, social and economic impacts • Detail how the traffic implications of the development will be managed, including details of the Travel Plan co-ordinator, the management arrangements for the plan and the development timetable

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
27	Travel Plan	National Planning Policy Framework paragraph 36 Plan for Stafford Borough: Policy T1	A Travel Plan will be required if the development is likely to generate significant amounts of traffic movement.	<p>Include</p> <ul style="list-style-type: none"> • activities for marketing and promotion of the plan to occupiers, users , visitors and residents of the site <p>Where an application requires a Travel Plan, applicants need to have agreed this before the application is made. If a complete Travel Plan is not submitted, the application will not be validated.</p> <p>Where an application requires a Travel Plan, the principle of this must be agreed with Staffordshire County Council Highways before the application is made.</p> <p>Further Advice</p> <p>Staffordshire County Council Highways: 0300 111 8000 highways@staffordshire.gov.uk Department for Transport: https://www.gov.uk/government/organisations/department-for-transport Department for Transport Good Practice Guidelines: Delivering Travel Plans Through the Planning Process (April 2009). Department for Transport: Making Residential Travel Plans Work (2007)</p>
28	Tree Survey / Assessment	National Planning Policy Framework paragraph 118	Any application where there are trees on the application site or on land adjacent to it (including street trees) that could be affected by or influence the development	<p>Information must be provided that details which trees are to be retained and how they will be protected during construction works.</p> <p>Full guidance on the survey information, tree protection plan,</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
28	Tree Survey / Assessment (continued)	Plan for Stafford Borough: Policy N5		<p>method statement and other information that should be provided with an application is set out in the current British Standard 5837 'Trees in relation to design, demolition and construction – Recommendations'. Using the methodology set out in the British Standard will help to ensure that development is suitably integrated with trees and that potential conflicts are avoided. The information should be prepared by a suitably qualified and experienced arboriculturalist.</p> <p>Further Advice Stafford Borough Council Tree Officer: 01785 619 539</p>
29	Ventilation / Extraction Statement	<p>Noise Policy Statement for England March 2010</p> <p>National Planning Policy Framework paragraphs 123</p> <p>Plan for Stafford Borough: Policy N1</p>	<p>All applications for the use of premises for the purposes within use classes:</p> <p>A3 (restaurants and cafes – use for the sale of food and drink for consumption on the premises)</p> <p>A4 (drinking establishments: public house, wine-bar or other drinking establishment)</p> <p>A5 (hot food takeaways – use for the sale of hot food for consumption off the premises)</p> <p>B2 (general industrial)</p>	<p>The statement for the method of ventilation / extraction must include:</p> <ul style="list-style-type: none"> • Elevations to show position, location and height (if external) • Proposed external finishes and fixings • Manufacturers specifications, including maintenance requirements • Silencing arrangements • Means of vibration isolation • Extraction fan acoustic performance, including noise emissions of sound power, and sound pressure levels, and narrow band and / or one third octave band frequency spectra • Predicted odour and / or particulate concentration

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
29	Ventilation / Extraction Statement (continued)			<p>Further Advice</p> <p>Stafford Borough Council Environmental and Health Services: 01785 619 402</p> <p>Guidance on the Control of Odour and noise from Commercial Kitchen Exhaust Systems (DEFRA) January 2005</p>
30	Viability Assessment	National Planning Policy Framework paragraph 173, 174, 177, 205	Where developers state that standard planning obligations as set out in The Plan for Stafford Borough will not be met	<p>The assessment should be based on an 'open book' approach and include the following:</p> <ul style="list-style-type: none"> • Purchase cost of the application site and when it was purchased • Detailed cost of construction, including any abnormalities and off site infrastructure • Predicted sale value / income from the finished site • Cost of Section 106 including affordable housing costs • % profit on cost both with and without the full Section 106 obligations <p>Further Advice Stafford Borough Council Development Management: 01785 619 337</p>
31	Water Quality Statement	National Planning Policy Framework paragraph 99 Plan for Stafford Borough: Policy N1, N2	All planning applications likely to have a detrimental impact on water quality	<p>The statement must explain how the development will not have a detrimental impact on water quality, either directly through pollution of surface water or indirectly through overloading of Wastewater Treatment Works.</p> <p>Further site specific analysis of any development proposals located in proximity or upstream of environmental significant sites, including Sites of Special Scientific Interest (SSSIs) and European</p>

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Validation Reference	Document	Policy Driver	Types of application that need this information	What information is required and where to look for more advice
31	Water Quality Statement (continued)	Habitat Directive 92/43/EEC – Conservation of Natural Habitats of Wild Fauna and Flora EU Water Framework Directive Habitat Regulations 2012		Sites, will be required to demonstrate that the development will not have an adverse effect on environmentally significant sites. Further Advice Section 4.3 of the Southern Staffordshire Outline Water Cycle Study and the Strategic Flood Risk Assessment update 2014



Householder Planning Applications

Information Checklist

Before you send us your application, make sure the following checklist is complete. Unless you are sending your application to us electronically, we will need 3 copies of each document.

Type of Information	What you need to do	Have you done this? (Yes, No or Not Applicable)
Application form	Complete all sections	
	Accurately describe what you are applying for	
	Complete the Declaration	
Certificates	Complete Certificate A if you are the owner of the land	
	Complete Certificate B and Notice 1 if someone else owns all or part of the land	
	Complete the Agricultural Holdings certificate	
Fee	Pay £172 to Stafford Borough Council (unless an exemption applies – see our Fees guide for more information)	
Location Plan	Use a scale of 1:1250 or 1:2500	
	Make sure it's up to date, if it's Ordnance Survey based it must display a copyright license	
	Draw a red line around the edge of all the land affected by the development (including access)	
	Draw a blue edge around all other land that you own	

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Type of Information	What you need to do	Have you done this? (Yes, No or Not Applicable)
Site/Block Plan	Use a scale of 1:100, 1:200 or 1:500	
	Make sure the direction of North is shown	
	Show the development in relation to property boundaries	
	Show the car parking layout, if this is new or changes to what's there now	
	Show any trees within the site boundary or next to it	
Floor Plans	Use a scale of 1:200, 1:100 or 1:50	
	Include existing plans and what it proposed	
	If existing car parking is affected, full floor plans of the whole property need to be shown	
Elevations	Use a scale of 1:200, 1:100 or 1:50	
	Include all the elevations (sides) of what you want to do	
	Include what the elevations look like now and what is proposed	
Flood Risk Assessment	Include an assessment if the property is within Flood Zone 2 or 3	
	Complete the Environment Agency template: www.environment-agency.gov.uk	
Ecological Report	Include a report on bats if a building likely to house bats is going to be demolished or a tree likely to provide foraging for bats is to be removed	
	Include a report on Great Crested Newts if ponds are involved	

**Stafford Borough Council Planning Application Local Validation Criteria
August 2017**

Type of Information	What you need to do	Have you done this? (Yes, No or Not Applicable)
Trees	Information is needed where there are trees on the application site or on land adjacent to it (including street trees) that could be affected by or that influence the development. The information that must be provided should detail which trees are to be retained and how they will be protected during construction works, in accordance with British Standard 5837 'Trees in relation to design, demolition and construction – Recommendations'. The information should be prepared by a suitably qualified and experienced arboriculturalist (tree specialist)	

Further information will be required where the proposal is within the curtilage of a Listed Building or involves demolition within a Conservation Area.

If you have any questions or need any help with your application for Householder development, please call our Planning Technicians on 01785 619 541, 01785 619 568 or email planningtechnicians@staffordbc.gov.uk

Application for Grant Aid 2017



Name of organisation:	
AEDdonate – Coppice Estate, Stone – Community Public Access Defibrillator Campaign	
Address: First Floor Offices 69 High Street Stone Staffordshire	Contact name: Jamie Richards
	Contact telephone no: 01785 472 224
	Contact email address: j.richards@aeddodate.org.uk
Amount of grant requested: £500	Total cost of project (if appropriate): £1,999
Reason for grant request:	
<p>AEDdonate is a charitable organisation who help communities and businesses fundraise and install their own Community Public Access Defibrillator. (CPAD).</p> <p>The Coppice Estate have identified the need for an external defibrillator to be installed <u>estate side</u> should a member of the community or visitor suffer a Sudden Cardiac Arrest (SCA) and the crossing barriers be down. As there is no alternative route onto the estate it would mean that the local ambulance service would not be able to access the patient and <u>any</u> delay would have a serious impact on the patients chances of survival.</p> <p>Having early access to a community defibrillator can increase a patient's chances of survival to over 75% from 6% if no community defibrillator is available. Cardiac arrest is Britain's biggest killer currently claiming over 100,000 lives across the UK each year; 620 of these being under the age of 35 and 270 being children.</p> <p>Having the defibrillator installed means that, through its link to the Local Ambulance Service it is available to the local community 24/7.</p> <p>We are seeking donations towards the defibrillator we are installing and as such contacting local businesses and organisations in the hope that they would be happy and willing to support the campaign. There will be recognition for all businesses who support the campaign which will be disseminated to the wider public.</p>	

Benefits to Stone residents:

The Community Public Access Defibrillator will benefit the local community and its visitors as a whole – young and old by making it more heart safe in the event of a SCA.

Unfortunately, we can't have an ambulance on every street corner and response times are on average 8 minutes to a Red 1 ambulance call (Cardiac Arrest).

Cardiac arrest is Britain's biggest killer currently claiming over 100,000 lives across the UK each year; 620 of these being under the age of 35 and 270 being children.

Cardiac Arrests are never going to stop -- We can however place the equipment into each community to give that patient a fighting chance of survival.

Other sources of funding secured or being explored (with amounts where known):

Network Rail and Virgin Trains have also been contacted along with Stone Festival to seek support and assistance with the campaign. Virgin Trains have donated two Standard Class complimentary train journeys anywhere on the Virgin Trains West Coast network and a response is awaited from Network Rail.

The Coppice Estate are also exploring self-fundraising opportunities within the community such as raffle, street party, etc with the assistance of AEDdonate.

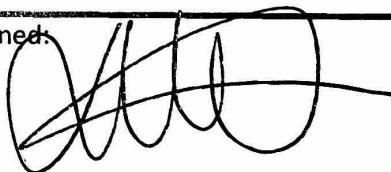
Is this an "exceptional" request (see notes)? If so, please explain why the Council should treat it as an exception:

Due to the location of Coppice Estate, Stone, Staffordshire and the fact that it is cut off from the emergency services when the train barriers are down it is vital that a Community Public Access Defibrillator is installed as a matter of urgency in order to keep the community heart safe.

In submitting this application, I confirm that it is put forward with the full knowledge and approval of the submitting organisation, and agree that its contents may be made available to the public and that the application and any communications relating to it may be stored in a computerised system.

I confirm that I have read the "Notes for Grant Applications 2017" document. I have enclosed the organisation's most recent set of accounts and, where appropriate, a statement providing details of how grants made previously have been spent and a statement of support from the Council's representative on the Management Committee

Signed:



Name: Jamie Richards

Position in organisation: Chief Executive

**AED DONATE
ACCOUNTS
FOR THE PERIOD ENDED 31 JULY 2016**



AED DONATE

CONTENTS

	Page
Independent Examiner's Report	1-2
Trustees' Annual Report	3-8
Receipts and payments	9-10



Independent examiner's report on the accounts

Section A Independent Examiner's Report

Report to the trustees/ members of	Charity Name AED DONATE		
On accounts for the year ended	31 JULY 2016	Charity no (if any)	1162634
Set out on pages	3 - 10 <small>(remember to include the page numbers of additional sheets)</small>		

Respective responsibilities of trustees and examiner

The charity's trustees are responsible for the preparation of the accounts. The charity's trustees consider that an audit is not required for this year under section 144 of the Charities Act 2011 (the Charities Act) and that an independent examination is needed.

It is my responsibility to:

- examine the accounts under section 145 of the Charities Act,
- to follow the procedures laid down in the general Directions given by the Charity Commission (under section 145(5)(b) of the Charities Act, and
- to state whether particular matters have come to my attention.

Basis of independent examiner's statement

My examination was carried out in accordance with general Directions given by the Charity Commission. An examination includes a review of the accounting records kept by the charity and a comparison of the accounts presented with those records. It also includes consideration of any unusual items or disclosures in the accounts, and seeking explanations from the trustees concerning any such matters. The procedures undertaken do not provide all the evidence that would be required in an audit, and consequently no opinion is given as to whether the accounts present a 'true and fair' view and the report is limited to those matters set out in the statement below.

Independent examiner's statement

In connection with my examination, no matter has come to my attention (other than that disclosed below *)

1. which gives me reasonable cause to believe that in, any material respect, the requirements:
 - to keep accounting records in accordance with section 130 of the Charities Act; and
 - to prepare accounts which accord with the accounting records and comply with the accounting requirements of the Charities Act have not been met; or
2. to which, in my opinion, attention should be drawn in order to enable a proper understanding of the accounts to be reached.

** Please delete the words in the brackets if they do not apply.*

Signed: Date: 24/5/2017

Name: MATTHEW JORDAN

Relevant professional qualification(s) or body (if any): FCCA

Address: DJH ACCOUNTANTS LIMITED, PORTHILL LODGE, HIGH STREET
WOLSTANTON, NEWCASTLE UNDER LYME
STAFFORDSHIRE, ST5 0EZ

Section B

Disclosure

Only complete if the examiner needs to highlight material problems.



Trustees' Annual Report for the period

Period start date: From Day 13 Month 07 Year 2015 To Day 31 Month 07 Year 2016

Section A Reference and administration details

Charity name: AED DONATE

Other names charity is known by:

Registered charity number (if any): 1162634

Charity's principal address: 69A HIGH STREET
STONE
STAFFORDSHIRE
Postcode: ST15 8AD

Names of the charity trustees who manage the charity

	Trustee name	Office (if any)	Dates acted if not for whole year	Name of person (or body) entitled to appoint trustee (if any)
1	Sarah Camacho		Appointment date: 19/02/2016	
2	John Scott		Appointment date: 01/09/2015	
3	Phyllis Richards		Appointment date: 20/07/2016	
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Names of the trustees for the charity, if any, (for example, any custodian trustees)

Name	Dates acted if not for whole year

Names and addresses of advisers (Optional information)

Type of adviser	Name	Address

Name of chief executive or names of senior staff members (Optional information)

--

Section B Structure, governance and management

Description of the charity's trusts

Type of governing document (eg. trust deed, constitution)	Constitution
How the charity is constituted (eg. trust, association, company)	Charitable incorporated organisation
Trustee selection methods (eg. appointed by, elected by)	Resolution passed at the meeting of the charity trustees

Additional governance issues (Optional information)

You **may choose** to include additional information, where relevant, about:

- policies and procedures adopted for the induction and training of trustees;
- the charity's organisational structure and any wider network with which the charity works;
- relationship with any related parties;
- trustees' consideration of major risks and the system and procedures to manage them.

--

Section C Objectives and activities

Summary of the objects of the charity set out in its governing document

For the public benefit the relief of sickness and preservation of good health by the provision of automated external defibrillators (AED's) and first aid training where applicable in public areas across the UK.

Summary of the main activities undertaken for the public benefit in relation to these objects (include within this section the statutory declaration that trustees have had regard to the guidance issued by the Charity Commission on public benefit)

The two key principles of public benefit issued by the Charity Commission namely ;

- There must be identifiable benefit or benefits .
- Benefits must be to the public or section of the public

Provide the framework through which AEDdonate undertake their activities.

AEDdonate is a charity that was formed to place public access defibrillators into communities AEDdonate provide the right support to communities when placing such specialised equipment and to also make sure the relevant links are made with each UK ambulance trust when placing AEDs into communities. This is vital for deployment to a patient that needs the use of a defibrillator.

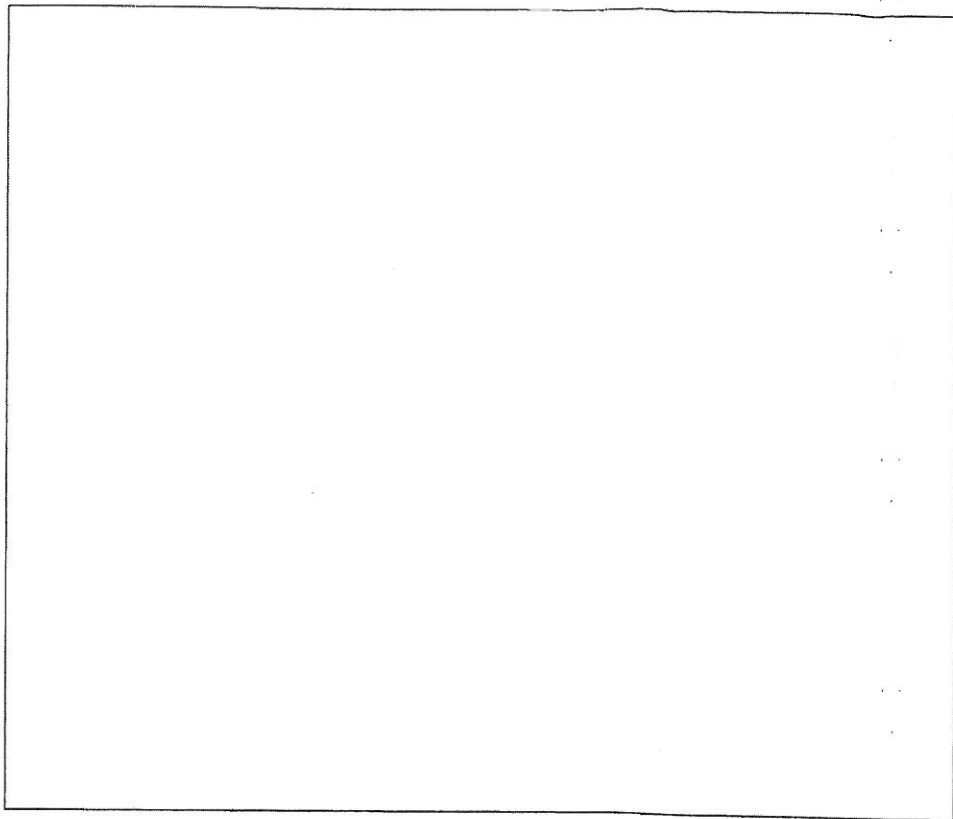
So far AEDdonate have saved over ten lives with our public access defibrillators and will continue to place AEDs into communities. Once a defibrillator is placed, AEDdonate carry out training sessions direct within the community. This provides the community with basic knowledge of CPR and ensures of how AED's are deployed.

AEDdonate have also opened a community facility within the building which enables us to provide training sessions to our local community, hold events and volunteer evenings. This is also available for use by local community groups which enable AEDdonate to engage with other agencies.

Additional details of objectives and activities (Optional information)

You **may choose** to include further statements, where relevant, about:

- policy on grantmaking;
- policy programme related investment;
- contribution made by volunteers.



Section D

Achievements and performance

Section D

Achievements and performance

Summary of the main achievements of the charity during the year

AEDdonate have placed over 800 defibrillators into communities across the UK. All AEDs are registered with UK. Ambulance trusts so they can be deployed to patients when required.

Over 20,000 people were trained on basic life support and AED training through community based training sessions by AEDdonate within the year.

AEDdonate have opened a community facility for local community groups to use within the building.

AEDdonate have successfully organised 2 charity balls to raise funds to place AEDs into local community.

AEDdonate have worked in partnership with a local brewery to create a charity beer. So far the monies raised from this have helped towards pub fundraising campaigns for AEDs within local community.

Our Charity have launched and working towards a volunteer team to promote the work we do further into other communities.

AEDdonate provide AEDs to local events to ensure each event has the appropriate equipment in place for medical emergencies.

Section E

Financial review

Brief statement of the charity's policy on reserves

At AEDdonate all funds received into the charity are placed straight back out into the community for defibrillators. Therefore AEDdonate does not hold any reserves at the moment. AEDdonate is working towards a reserve account in the future.

Details of any funds materially in deficit

N/A

Further financial review details (Optional information)

You may choose to include additional information, where relevant about:

- the charity's principal sources of funds (including any fundraising);
- how expenditure has supported the key objectives of the charity;
- investment policy and objectives including any ethical investment policy adopted.

Section F

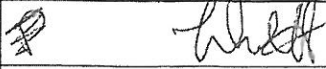
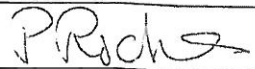
Other optional information

Section G

Declaration

The trustees declare that they have approved the trustees' report above.

Signed on behalf of the charity's trustees

Signature(s)		
Full name(s)	JOHN Darren SCOTT	PHILLIS MARGARET RICHARDS
Position (eg Secretary, Chair, etc)		
Date	11.5.17	



CHARITY COMMISSION
FOR ENGLAND AND WALES

Charity Name
AED DONATE

No (if any)
1162634

CC16a

Receipts and payments accounts

For the period from	Period start date 13/07/2015	To	Period end date 31/07/2016
------------------------	---------------------------------	----	-------------------------------

Section A Receipts and payments

	Unrestricted funds to the nearest £	Restricted funds to the nearest £	Endowment funds to the nearest £	Total funds to the nearest £	Last year to the nearest £
A1 Receipts					
DONATIONS, LEGACIES AND GRANTS	72,143	-	-	72,143	-
FUNDRAISING EVENTS	7,452	-	-	7,452	-
	-	-	-	-	-
	-	-	-	-	-
	-	-	-	-	-
	-	-	-	-	-
<i>Sub total (Gross income for AR)</i>	79,595	-	-	79,595	-
A2 Asset and investment sales, (see table).					
	-	-	-	-	-
	-	-	-	-	-
<i>Sub total</i>	-	-	-	-	-
Total receipts	79,595	-	-	79,595	-
A3 Payments					
LABOUR	32,745	-	-	32,745	-
HARDWARE COSTS	24,911	-	-	24,911	-
CARRIAGE	1,739	-	-	1,739	-
COST OF FUNDRAISING EVENTS	10,249	-	-	10,249	-
PROFESSIONAL FEES	1,100	-	-	1,100	-
MEDICAL COVER	3,829	-	-	3,829	-
TRAINING	750	-	-	750	-
TRAVELLING EXPENSES	487	-	-	487	-
BANK AND TRANSACTION CHARGES	105	-	-	105	-
PRINTING, POSTAGE, STATIONERY AND COMPUTER COSTS	3,584	-	-	3,584	-
<i>Sub total</i>	79,499	-	-	79,499	-
A4 Asset and investment purchases, (see table)					
	-	-	-	-	-
	-	-	-	-	-
<i>Sub total</i>	-	-	-	-	-
Total payments	79,499	-	-	79,499	-
<i>Net of receipts/(payments)</i>	96	-	-	96	-
A5 Transfers between funds	-	-	-	-	-
A6 Cash funds last year end	-	-	-	-	-
<i>Cash funds this year end</i>	96	-	-	96	-

Section B Statement of assets and liabilities at the end of the period

Categories	Details	Unrestricted funds to nearest £	Restricted funds to nearest £	Endowment funds to nearest £
B1 Cash funds	BANK ACCOUNT	96	-	-
		-	-	-
		-	-	-
	Total cash funds	96	-	-
(agree balances with receipts and payments account(s))		OK	OK	OK

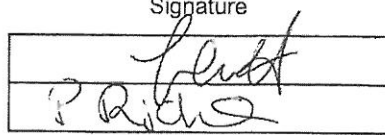
Categories	Details	Unrestricted funds to nearest £	Restricted funds to nearest £	Endowment funds to nearest £
B2 Other monetary assets		-	-	-
		-	-	-
		-	-	-
		-	-	-
		-	-	-
		-	-	-

Categories	Details	Fund to which asset belongs	Cost (optional)	Current value (optional)
B3 Investment assets			-	-
			-	-
			-	-
			-	-
			-	-

Categories	Details	Fund to which asset belongs	Cost (optional)	Current value (optional)
B4 Assets retained for the charity's own use			-	-
			-	-
			-	-
			-	-
			-	-
			-	-
			-	-
			-	-

Categories	Details	Fund to which liability relates	Amount due (optional)	When due (optional)
B5 Liabilities			-	
			-	
			-	
			-	
			-	

Signed by one or two trustees on behalf of all the trustees

Signature  P Richards	Print Name JOHN SCOTT PHYLLIS RICHARDS	Date of approval 11.5.17 11.5.17
--	--	--

Stone Town Council - Non-Cheque Payments

The table below lists all non-cheque payments made by the Council in the period since the last report, for the Committee's information.

The table includes payments by direct debit, telephone banking and online banking. It excludes salary and related payments, payments from the Mayor's Charity, and transfers between the Council's bank accounts. These excluded items can be seen by any Member on request.

Date	Reference	Supplier	Description	Amount
03/07/2017	D/Dbt	SBC	Rates - Northesk Street Car Park	£105.00
03/07/2017	D/Dbt	SBC	Rates - Crown Street Car Park	£241.00
03/07/2017	D/Dbt	Vouchers charges	Voucher charges	£19.50
03/07/2017	D/Dbt	SBC	Rates - Stone Station Community Centre	£210.00
03/07/2017	D/Dbt	SBC	Rates - Market Square	£237.00
03/07/2017	D/Dbt	SBC	Rates - Frank Jordan Centre	£405.00
03/07/2017	D/Dbt	British Gas	Electricity charges - Stone Station Community Centre	£351.04
03/07/2017	Tele/Bank	Panda Press Stone	Music Festival & Late Night Posters	£312.00
03/07/2017	Tele/Bank	Panda Press Stone	Civic Sunday - Order of Service	£259.00
04/07/2017	D/Dbt	Francotyp Postalia	Postage	£200.00
07/07/2017	D/Dbt	EE & T Mobile	Caretakers phone	£24.41
13/07/2017	D/Dbt	British Gas	Electricity charges - Frank Jordan Centre	£454.78
27/07/2017	D/Dbt	British Gas	Gas supply - Stone Station Community Centre	£48.02
31/07/2017	D/Dbt	Bank charges	Bank charge	£51.03
01/08/2017	D/Dbt	Bank charges	Voucher charges	£19.50
01/08/2017	Tele/Bank	Printdesigns Ltd	Banners for late night shopping	£89.67
03/08/2017	D/Dbt	SBC	Rates - Crown Street Car Park	£241.00
03/08/2017	D/Dbt	SBC	Rates - Northesk Street Car Park	£105.00
03/08/2017	D/Dbt	SBC	Rates - Stone Station Community Centre	£210.00
03/08/2017	D/Dbt	SBC	Rates - Market Square	£237.00
03/08/2017	D/Dbt	SBC	Rates - Frank Jordan Centre	£405.00
07/08/2017	D/Dbt	EE & T Mobile	Caretakers phone	£17.65
31/08/2017	D/Dbt	Bank charges	Bank charge	£82.06