Isle of Anglesey County Council

Data Protection Policy

Version 2.0 (March 2020)

About this policy

Isle of Anglesey County Council is fully committed to compliance with the requirements of the Data Protection Legislation

The Council will therefore follow procedures which aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties under the Data Protection Legislation

The Policy is supported by resources on the Council's website.

Revision history

Version	Date	Summary of changes
1.0	May 2018	New Policy
2.0	March 2020	Minor amendments made following a review.

Date of next review	
This policy will be reviewed in:	March 2022
The review will be undertaken by:	Data Protection Officer

Contact Details: The Data Protection Officer
dpo@anglesey.gov.uk
01248 751806

We are happy to provide this policy in alternative formats on request. Please use the above contact details.

Mae'r ddogfen yma ar gael yn y Gymraeg.

This document is available in Welsh.

Data Protection Policy

1. **Policy Statement**
2. **Scope**
3. **Definitions**
4. **Data Protection Principles**
5. **Basis for Processing Personal Information**
6. **Sensitive Personal Information**
7. **Criminal Records Information**
8. **Data Protection Impact Assessments (DPIAs)**
9. **Documentation and records**
10. **Privacy Notice**
11. **Individual rights**
12. **Individual obligations**
13. **Information Security**
14. **Storage, retention and Personal Information**
15. **Data Breaches**
16. **Internal Data Transfers**
17. **Training**
18. **Consequences of failing to comply**

You must read this policy because it gives important information about:

- the data protection principles with which Anglesey County Council must comply;
- what is meant by personal data and special categories of personal data;
- how we gather, use and (ultimately) delete personal data and special categories of data in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal data we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

1.POLICY STATEMENT

1.1 Isle of Anglesey County Council is fully committed to compliance with the requirements of The General Data Protection Regulation which came into force on 25 May 2018. This policy also relates to the following legislative requirements incumbent on the Council:

- Local Government Act 1972
- Local Government (Access to Information) Act 1985
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Re-use of Public Sector Information Regulations 2005

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff members understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

1.4 The Council's Data Protection Officer, is responsible for informing and advising the Council and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Council's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Protection Officer.

1.5 Any breach of this policy will be taken seriously and may result in disciplinary action and financial sanctions.

1.6 In order to operate efficiently, the Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees and or workers, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

1.7 This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

1.8 The Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those for whom it provides / arranges services and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

2.SCOPE

2.1 This policy applies to the personal information of job applicants, current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices, clients, customers, and suppliers.

2.2 Staff should refer to Anglesey County Council's Data Protection Policy and, where appropriate, to other relevant guidance and policies including in relation to internet, email and communications, monitoring, social media, information security, data retention, and criminal record information, which contain further information regarding the protection of personal information in those contexts.

2.3 We will review and update this policy regularly in accordance with our data protection obligations. It does not form part of any employee's contract of employment. We may amend, update or supplement it from time to time and we will circulate any new or modified policy to staff when it is adopted.

2.4 Some of the responsibilities within this policy extend to employees of the Council beyond their period of employment or to elected Members beyond their period of office. This paragraph refers specifically to their continued responsibility to keep secure and not publicly disclose the personal data of any third party (particularly any sensitive personal information) to which they may have had privileged access by virtue of their period of employment or office.

3.DEFINITIONS

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal data	means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
A joint data controller	where two or more controllers jointly determine the purpose and means of processing. This situation may arise where

	the Council is collecting the data on behalf of a larger regional or pan-Wales partnership.
special categories of personal data	means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

3.1 Data is information which is stored electronically, on a computer, or in paper-based filing systems.

3.2 Data controllers are the people, or organisations, which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. Anglesey Council is the data controller of all personal data used in our Authority.

3.3 Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.4 Data processors include any person who processes personal data on behalf of a data controller (other than an employee of the data controller). As noted above, the Council is the data controller and therefore employees of the Council are excluded from this definition. Data Processors therefore could include suppliers which handle personal data on our behalf.

4.DATA PROTECTION PRINCIPLES

4.1 The Council will implement technical and organisational measures to manifest that it has considered and integrated data protection into all its processing activities, in accordance with the applicable data protection principles, laws and rights of individuals as set out below in this section. The Council's approach to data protection will be, as required by GDPR, 'data protection by design and default' and 'privacy by design

4.2 The Council will comply with the following data protection principles when processing personal information:

4.2.1 we will process personal data lawfully, fairly and in a transparent manner;

4.2.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.2.3 we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;

4.2.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

4.2.5 we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

4.2.6 we will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

4.3 There is furthermore an overarching principle of accountability which means that the Council must not only comply with the six GDPR principles but must be seen to be complying with them in its public face and be able to demonstrate compliance if inspected by regulatory bodies, such as the ICO.

4.4 First GDPR principle: fair and lawful processing;

4.4.1 Processing of personal data must only be undertaken where the Council has a lawful basis

4.4.2 for carrying out the activity. GDPR specifies six lawful bases for processing, as follows:

1) Processing is necessary for compliance with a legal obligation to which the controller is subject. This is applicable to all statutory services which the Council is obliged to provide.

2) 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. This is applicable to all services where the Council is empowered but not obliged to provide a service by legislation (for example the provision of council housing).

3) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

4) Processing is in the vital interests of the data subject.

5) Processing is in the Council's legitimate interests and does not unduly prejudice the individual's privacy. This is applicable only to internal services such as Payroll and HR and cannot be applied to the Council's public task.

6) The data subject has given consent to the processing of his or her personal data for one or more specific purposes. This is applicable mostly to marketing activity.

4.5 Second GDPR principle: specified and legitimate purposes

4.5.1 When gathering personal data or establishing new data protection activities, staff should ensure that data subjects receive appropriate privacy notices to inform them how the data will be used. There are limited exceptions to this requirement, which are specified in GDPR.

4.5.2 A 'privacy notice' is a statement that explains some or all of the ways an organisation gathers, uses, discloses, and manages the personal data it collects from its customers or clients. It fulfils part of the

organisation's legal requirement to respect a customer or client's privacy when collecting and sharing personal data.

4.6 Third GDPR principle: adequate, relevant and limited

4.6.1 Staff should make sure data processed by them is adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should not generally be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

4.7 Fourth GDPR principle: accuracy

4.7.1 Individuals may ask the Council to correct personal data relating to them which they consider to be inaccurate. If a member of staff receives such a request and does not agree that the personal data held is inaccurate, they should nevertheless record the fact that it is disputed and inform the Data Protection Officer (DPO).

4.8 Fifth GDPR principle: retention only as long as necessary

4.8.1 Personal data should not be retained for any longer than necessary. Staff should follow the corporate records retention schedule for guidance. The length of time for which data should be retained may vary from this schedule depending upon particular circumstances, including any special reasons why it was obtained.

4.9 Sixth GDPR principle: security

4.9.1 Staff must keep personal data secure against loss or misuse in accordance with the ICT Security Policy Framework. Where the Council uses external organisations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal data. Staff should consult the DPO to discuss the necessary steps to ensure compliance when setting up any new data processing agreement or altering any existing agreement.

5. Compliance with Individuals rights under GDPR

5.1 The General Data Protection Regulation (GDPR) gives individuals several rights regarding their personal information.

5.2 The Council will implement a set of rules and procedures, creating a workflow for the evaluation of requests, with regard to the following individual rights under GDPR:

5.2.1 The right to be informed

5.2.1.1 The Council will explain at the point of collection how it intends to use the data it is collecting, whether it will share the data with anyone else, what is the legal basis for processing and which individuals' rights apply. The primary method for communicating this information will be corporate privacy note supplemented by

brief privacy statement at the point of collection which reference amongst other things the full notice.

5.2.1.2 Other versions of the privacy notice will complement it, suitable for explaining the concepts of privacy and data protection to children and to others who may reasonably expect the information to be available in other, more accessible formats.

5.2.2 The right of access

5.2.2.1 Individuals are entitled (subject to certain exemptions specified in the Data Protection Act) to request access to information held about them. All such Subject Access Request should be logged at a corporate level and referred onward immediately to the relevant officer(s) for action. Timeliness is particularly important because the Council must respond to a valid request within legally prescribed time limits.

5.2.3 The right to rectification

5.2.3.1 Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. The Council must respond within one month to any reasonable request for rectification, although this can be extended by two months where the request for rectification is complex. If the Council has shared the personal data in question with other agencies, each agency must be informed and asked to make the same rectification - unless this proves impossible or involves disproportionate effort. If asked to, staff must also inform the data subjects about these agencies whose data may also be inaccurate.

5.2.3.2 If the request for rectification is refused (for example where the data subject's authenticity is contested), staff must explain why to the individual, informing them of their right of appeal to the DPO and to seek a judicial remedy.

5.2.4 The right to restrict processing

5.2.4.1 Individuals are entitled to block the processing of their personal data in certain circumstances. The data may continue to be stored but processing of it must cease.

5.2.4.2 The Council is only required to restrict the processing of personal data in the following circumstances: where an individual contests the accuracy of the personal data; where following an objection to processing the Council is considering whether its legitimate grounds override those of the individual (this is only applicable where the legal basis for processing is either performance of the public task or the exercise of

legitimate interests, see 6.2 below); when processing is unlawful and the individual opposes erasure and requests restriction instead; if the Council no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

5.2.5 The right to object to processing

5.2.5.1 Where the legal basis for processing is performance of a public task or the exercise of legitimate interests, individuals have the right to object to processing, including any profiling based on those provisions. The Council shall no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

5.2.5.2 Where the legal basis for processing is consent, individuals have an absolute right to object to the Council processing their data for this purpose, to which demand staff must immediately respond without question. This legal basis for processing and this right applies in particular to any direct marketing undertaken by the Council, for example marketing for its cultural, leisure and other discretionary/optional services.

5.2.6 Rights on automated decision making and profiling

5.2.6.1 Individuals have the right to be informed when their data is subject to automated decision making and profiling. The Council does not currently carry out such activity, hence the condition does not apply at present. A note to this effect is contained in the privacy notice.

5.2.7 Right to data portability

5.2.7.1 Individuals have the right to demand that their personal data is transferred to another agency (for example when moving to another area). 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. This limited right only applies where the legal basis for processing is performance of a contract or based on consent, hence is not applicable in any great degree to local authorities.

5.2.8 Right to erasure or ‘right to be forgotten’

5.2.8.1 Individuals also have the right, in the case of reliance on consent, to demand that their personal data be removed entirely from the particular processing activity, the so-called ‘right to be forgotten’. This limited right applies mostly to direct marketing activity by the Council.

6.BASIS FOR PROCESSING PERSONAL DATA

6.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

6.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

6.1.1.1 that the data subject has consented to the processing;

6.1.1.2 that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

6.1.1.3 that the processing is necessary for the protection of the vital interests of the data subject or another natural person;

6.1.1.4 that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority;

6.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

6.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

6.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

6.1.5 where special categories of data are processed, also identify a lawful special condition for processing that information and document it; and

6.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

6.2 When determining whether Anglesey County Council's legitimate interests are the most appropriate basis for lawful processing, we will:

6.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

6.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

6.2.3 keep the LIA under review, and repeat it if circumstances change; and

6.2.4 include information about our legitimate interests in our relevant privacy notice(s).

7 SPECIAL CATEGORIES OF PERSONAL DATA

7.1 Special categories of personal data' is sometimes referred to as Sensitive personal information 'or 'sensitive personal data'.

7.2 The Council may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

7.2.1 we have a lawful basis for doing so as set out above, e.g. it is necessary for the performance of the employment contract, to comply with the Council's legal obligations or for the purposes of the Council's legitimate interests; and

7.2.2 one of the special conditions for processing sensitive personal information applies, e.g:

7.2.2.1 the data subject has given explicit consent;

7.2.2.2 the processing is necessary for the purposes of exercising the employment law rights or obligations of the Council or the data subject;

7.2.2.3 the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

7.2.2.4 processing relates to personal data which are manifestly made public by the data subject;

7.2.2.5 the processing is necessary for the establishment, exercise or defence of legal claims; or

7.2.2.6 the processing is necessary for reasons of substantial public interest.

7.3 Before processing any sensitive personal information, staff must notify the Data Protection Officer of the proposed processing, in order that the Data Protection Officer may assess whether the processing complies with the criteria noted above.

7.4 Sensitive personal information will not be processed until:

7.4.1 the assessment referred to in paragraph 7.3 has taken place; and

7.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

7.5 The Council will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

7.6 The Council's *data protection Privacy Notices* set out the types of sensitive personal information that the Council processes by Service, what it is used for and the lawful basis for the processing

7.7 In relation to special categories of data, the Council will comply with the procedures set out in this policy to make sure that it complies with the data protection principles set out in paragraph 4 above.

7.8 **During the recruitment process**: the HR department, with guidance from the Data Protection Officer will ensure that (except where the law permits otherwise):

7.8.1 during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;

7.8.2 if sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

7.8.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

7.8.4 we will not ask health questions in connection with recruitment OR only ask health questions once an offer of employment has been made.

7.9 **During employment**: the HR department, with guidance from the Data Protection Officer will process:

7.9.1 health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

7.9.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and

7.9.3 trade union membership information for the purposes of staff administration and administering 'check off'.

8 CRIMINAL RECORDS INFORMATION

Criminal records information will be processed in accordance with the Council's policies and procedures.

9 DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

9.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the Council is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

9.1.1 whether the processing is necessary and proportionate in relation to its purpose;

9.1.2 the risks to individuals; and

9.1.3 what measures can be put in place to address those risks and protect personal information.

9.2 Before any new form of technology is introduced, the manager responsible should therefore contact the Data Protection Officer in order that a DPIA can be carried out.

9.3 During the course of any DPIA, the Service will seek the advice of the Data Protection Officer and the views of a representative group of employees and any other relevant stakeholders (where applicable).

10 DOCUMENTATION AND RECORDS

10.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

10.1.1 the name and details of the Service, Staff involved, (and where applicable, of other controllers and the Council's DPO);

10.1.2 the purposes of the processing;

10.1.3 a description of the categories of individuals and categories of personal data;

10.1.4 categories of recipients of personal data;

10.1.5 where possible, retention schedules; and

10.1.6 where possible, a description of technical and organisational security measures.

10.2 As part of our record of processing activities we document, or link to documentation, on:

10.2.1 information required for privacy notices;

10.2.2 records of consent;

10.2.3 controller-processor contracts;

10.2.4 the location of personal information;

10.2.5 DPIAs; and

10.2.6 records of data breaches.

10.3 If we process sensitive personal information or criminal records information, we will keep written records of:

10.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

10.3.2 the lawful basis for our processing; and

10.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

10.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

10.4.1 carrying out information audits to find out what personal information the Council holds;

10.4.2 distributing questionnaires and talking to staff across the Council to get a complete picture of our processing activities; and

10.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

10.5 We document our processing activities in electronic form so we can add, remove and amend information easily.

11. PRIVACY NOTICE

11.1 The Council will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

11.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

12. INDIVIDUAL RIGHTS

12.1 You (in common with other data subjects) may have the following rights in relation to your personal information:

12.1.1 to be informed about how, why and on what basis that information is processed—see the Council's Privacy Notice];

12.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the Council's Subject Access Request Policy;

12.1.3 to have data corrected if it is inaccurate or incomplete;

12.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

12.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the Council no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

12.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the Council is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

12.2 If you wish to exercise any of the data subject rights, please contact The Data Protection Officer.

13. INDIVIDUAL OBLIGATIONS

13.1 Individuals are responsible for helping the Council keep their personal information up to date. You should let *the HR department* know if the information you have provided to the Council changes, for example if you move house or change details of the bank or building society account to which you are paid. Alternatively, you can update your own personal information on a secure basis via the Council's intranet.

13.2 You may have access to the personal information of other members of staff, suppliers and customers or clients of the Council in the course of your employment or engagement. If so, the Council expects you to help meet its data protection obligations to those individuals.

13.3 If you have access to personal information, you must:

13.3.1 only access the personal information that you have authority to access, and only for authorised purposes;

13.3.2 only allow other Council staff to access personal information if they have appropriate authorisation;

13.3.3 only allow individuals who are not Council staff to access personal information if you have specific authority to do so from the Data Protection Officer;

13.3.4 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure

file storage and destruction and other precautions set out in the Council's IT security policy;

13.3.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Council's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

13.3.6 not store personal information on local drives or on personal devices that are used for work purposes**.**

13.4 You should contact the Data Protection Officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place);

13.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 7.2.2 being met;

13.4.2 any data breach as set out in paragraph 16 below;

13.4.3 access to personal information without the proper authorization;

13.4.4 personal information not kept or deleted securely;

13.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Council's premises without appropriate security measures being in place;

13.4.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4 above.

14 INFORMATION SECURITY

14.1 The Council will use appropriate technical and organisational measures in accordance with the Council's policies to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

14.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

14.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

14.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

14.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

14.2 Where the Council uses external organisations to process personal information on its behalf, additional security arrangements need to be

implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

14.2.1 the organisation may act only on the written instructions of the Council;

14.2.2 those processing the data are subject to a duty of confidence;

14.2.3 appropriate measures are taken to ensure the security of processing;

14.2.4 sub-contractors are only engaged with the prior consent of the Council and under a written contract;

14.2.5 the organisation will assist the Council in providing subject access and allowing individuals to exercise their rights in relation to data protection;

14.2.6 the organisation will assist the Council in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

14.2.7 the organisation will delete or return all personal information to the Council as requested at the end of the contract; and

14.2.8 the organisation will submit to audits and inspections, provide the Council with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Council immediately if it is asked to do something infringing data protection law.

14.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

15 STORAGE AND RETENTION OF PERSONAL INFORMATION

15.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Council's *IT security policy*.

15.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the Council's *Records Management Policy* which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult with the Data Protection Officer.

15.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

16 DATA BREACHES

16.1 A data breach may take many different forms, for example:

16.1.1 loss or theft of data or equipment on which personal information is stored;

16.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

16.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

16.1.4 human error, such as accidental deletion or alteration of data;

16.1.5 unforeseen circumstances, such as a fire or flood;

16.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

The Council will:

16.1.7 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

16.1.8 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

17 INTERNAL DATA TRANSFERS

17.1 The Council will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

17.2 If the Council does need to transfer personal information outside of the EEA, perhaps to the US for instance, the Council will use a Privacy Shield. The adequacy of this shield will be reviewed annually. This annual review should address the GDPR's requirement for a mechanism for a periodic review, at least once every four years, of relevant developments.

18 Monitoring of Compliance

18.1 The Council should follow this policy for all relevant processes and procedures in its operational activities. Effectiveness of the incorporation of the policy into departmental processes and procedures will be assessed at intervals through the process of internal audit and at the behest of the DPO, who may carry out an internal investigation without prior notice or consent should s/he have cause for concern. Such audits of service areas will, amongst other measures:

- Identify areas of operation within the service area that are covered or not covered by the policy and to identify any relevant processing and/or procedures which fail to adhere to the policy

- Demand that a Data Protection Impact Assessment be carried out immediately where current methods of data processing present a corporate risk (for example where large Version 2.0 - 02.10.2019 Page 12 of 12 quantities of sensitive personal data are being processed with potentially inadequate safeguards), or where a significant data breach has already occurred.
- Set requirements for implementing new operational procedures with regard to data protection, processing of data and dealing with requests for information.
- Highlight where non-conformance to the operational procedures is occurring and suggest a tightening of controls and adjustment to related procedures in the form of an improvement action plan

19. TRAINING

The Council will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

20. CONSEQUENCES OF FAILING TO COMPLY

20.1 The Council takes compliance with this policy very seriously. Failure to comply with the policy:

20.1.1 puts at risk the individuals whose personal information is being processed; and

20.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Council; and

20.1.3 may, in some circumstances, amount to a criminal offence by the individual.

20.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

20.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact The Data Protection Officer.