Midlothian Council
Privacy Policy

Policy Statement

1.1 This policy sets out Midlothian Council's (the Council) approach to managing personal data in accordance with the requirements of the General Data Protection Regulation (the 'GDPR').

1.2 A guiding principle for the Council in conducting its business is the protection of the fundamental rights and freedom of individuals and in particular, their right to privacy with respect to the processing of their personal data.

1.3 The Council needs to collect and use certain information about customers to allow us to carry out our many and varied functions and responsibilities. This personal information, however it is acquired, held, processed, released or destroyed must be dealt with lawfully and properly, and the Council will work within the terms of the GDPR in all its dealings with personal data.

1.4 The Council regards the appropriate treatment of personal information as central to our operations, and to maintaining the confidence of our customers. To that end we will foster a culture of awareness of the GDPR and its guiding principles.

Scope

2.1. This policy applies to:

2.1.2 All personal data held, maintained and used by the Council in all locations and in all media (hardcopy and electronic).

2.1.3 All Elected Members, Council staff, including Temporary staff, Contractors, Consultants and Volunteers that access and use Council information; and

2.1.4. All Third Parties that manage and process personal data on the Council's behalf when carrying out a statutory Council function or service.

Definitions

3.1 **Data Controller –** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data**.** This may be an individual or an organisation. Data Controllers can process personal data jointly with other data controllers for specified purposes. The Council is a data controller. Elected members are data controllers for the purposes of their constituency work;

3.2 **Data Processor** – is a person, other than an employee of the Council, who processes personal data on behalf of the Council. This processing must be evidenced in a written contract. The Data Processor can only use personal data under the instructions of the Council. Data Processors have the same data security obligations as the Council as a Data Controller.

3.3 The **'Act'** means the Data Protection Act 2018 passed by the UK Government to implement the GDPR, particularly in relation to derogated matters, and to provide a framework for Data Protection once the UK leaves the EU.

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

3.5 **Data Protection Officer** – is the person appointed by the Council pursuant to Article 37 of the GDPR.

3.6 **Data Subject** – is a living individual who can be identified from the personal data or from additional information held, or obtained, by the Council.

3.7 **European Economic Area** – includes member states of the European Union and three of the member states of the European Free Trade Association (Iceland, Liechtenstein and Norway).

3.8 **Enforcement Notice** – The Information Commissioner has the power to serve an Enforcement Notice on a Data Controller if he determines that a Data Controller has failed to comply with the requirements of the GDPR. The Notice sets out the actions that a Data Controller must take to achieve compliance. A Data Controller can lodge an appeal against the Notice to the Information Tribunal. It is a criminal offence for a Data Controller to fail to comply with a valid Enforcement Notice.

3.9 **GDPR** is the European Union General Data Protection Regulation 2016/679 of 27 April 2016 which came into effect on 25th May 2018 and provides a regime for the protection of personal data in relation to European citizens.

3.10 **Information Commissioner -** is an independent public authority regulator and the UK supervising authority responsible for ensuring all organisations comply with the GDPR. Organisations are required to notify personal data security breaches to the ICO if they breach the GDPR. The Commissioner has been granted enforcement powers regarding non-compliance, these include the ability to issue information and enforcement notices, and impose large fines (up to 20m Euros or 4% of global turnover, whichever is the greater). Further information about data protection is available on the Information Commissioner Office website at www.ico.org.uk

3.11 **Information Notice** – an Information Notice can be issued by the Information Commissioner which requires a Data Controller to provide his office with information that he requires to carry out his functions. Failure to comply with an Information Notice is a criminal offence.

3.12 **Information Security** – ensures that information or personal data held by the Council is not compromised by unauthorised access, modification, disclosure or loss.

3.13 **Information (or data) Sharing** – ensures that information or personal data held by the Council is shared in a compliant, controlled and transparent manner.

3.14 **Midlothian Joint Integration Board (MJIB)** – is responsible for delivering the Integration Scheme for the integration of Adult Health and Social Care. This is a joint enterprise between the Council, NHS Lothian, and the MJIB constituted under the Public Bodies (Joint Working) (Scotland) Act 2014.

3.15 **Personal data (or information)** – is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;. Examples of personal data are contained in paper files, electronic records and visual and audio recordings.

3.16 **Processing** – means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.17 **Sensitive personal data –** requires a higher level of consideration. Information will be considered 'sensitive personal data' if it relates to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or criminal offences or alleged criminal activity (including any criminal proceedings).

Policy content

Data Protection Principles

4.1 The Council needs to collect and use information about its customers to facilitate the effective delivery of services. The GDPR ensures that this information is gathered, used, stored, shared, protected, retained and destroyed in a way which is fair and lawful.

4.2 There are six Data Protection Principles which require that personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals; (**'the lawfulness, fairness and transparency principle'**).

(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; (**the purpose limitation principle'**).

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; ('**the data minimisation principle'**).

(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; (**the 'accuracy' principle'**).

(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; (**the 'storage limitation principle'**).

(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; (**the 'integrity and confidentiality principle'**).

4.3 In addition to the above the Council shall be responsible for, and be able to demonstrate, compliance with the above principles – for example by documenting the decisions taken in relation to processing activity (**the 'accountability principle'**).

Lawful processing

4.4 For processing to be lawful under the GDPR, the Council needs to identify a lawful basis before it can process personal data. These are often referred to as the "conditions for processing". It is important that the Council determines the lawful basis for processing personal data and documents this. See the Appendix for the main conditions for processing under the GDPR which will be further extended by the Act. If necessary, the Data Protection Officer should be consulted in order to clarify the legal basis for any processing.

4.5 The GDPR refers to sensitive personal data as "special categories of personal data". Personal data relating to criminal convictions and offences are not included, but similar extra safeguards in Article 10 apply to its processing.

4.6 One of the conditions for lawful processing is the consent of the data subject. Under GDPR consent 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 the Council needs to provide simple ways for people to withdraw consent. The Council must take care to ensure that consent is freely given. Moreover, consent has to be verifiable, and individuals generally have more rights where the Council relies on consent to process their data.

4.7 It is important to be aware that the Council can rely on other lawful bases apart from consent – for example, where 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 Council, as a Data Controller.

Children's Personal Data

4.8 The GDPR contains provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, the Council must ensure that our privacy notice, and any other documentation we produce relating to these types of processing activities are written in a clear, plain way that a child will understand.

4.9 If the Council offers an online service to children, we will need to obtain explicit consent from a parent or guardian to process the child's data. Parental/guardian consent for access to online services is required for children aged 13 and under.

4.10 Online Services includes most internet services provided at the user's request and 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.

4.11 Parental/guardian consent is not required where the processing is related to Preventative or Counselling Services offered directly to a child.

Privacy by Design and Default

4.12 Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start.

4.13 In terms of the GDPR the Council has an obligation to implement technical and organisational measures to prove that the Council has considered and integrated data protection into our processing activities. The Council will ensure that privacy and data protection is a key consideration in the early stages of any project which includes the following:

(a) building new systems for storing or accessing personal data;
(b) policy or strategies that have privacy implications;
(c) embarking on a data sharing initiative; or
(d) using data for new purposes**.**

Data Protection Impact Assessment

4.14 The Council regularly collects and processes personal data from individuals who receive services or have a relationship with the Council (e.g. suppliers, employees). However, the Council will only obtain, use and retain personal information that it actually needs to fulfil its business and operational requirements.

4.15 A Data Protection Impact Assessment (DPIA) will be completed when processes or services that involve personal data are designed or revised. The DPIA will identify and document appropriate governance controls required to manage the privacy risks associated with the process.

4.16 Specifically, a DPIA must be carried out when:

(a) using new technologies; and

(b) 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 sensitive personal data or personal data in relation to criminal convictions or offences; and
- large scale, systematic monitoring of public areas (CCTV).

4.17 DPIAs must be prepared by the relevant Service Manager in consultation with the Data Protection Officer. Once approved the DPIA will be registered with the Data Protection Officer..

Informing Data Subjects and Fair Processing

4.18 The GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These place an emphasis on the Council to ensure that privacy notices are understandable and accessible.

4.19 The Council must provide information to people about how it processes their personal data and it must be in a manner which is concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

4.20 Appropriate fair processing information will be provided at the time personal data is collected directly from data subjects or from a third party.

4.21 It is recognised that in order to provide customers with a better service and to fulfil the Council's statutory functions, personal data collected across Council services may be used in different ways, if its use is deemed appropriate and fair. In such cases, data subjects will be advised if their personal data is to be used in a new way.

4.22 Fair processing information must be approved by the Data Protection Officer and documented within the relevant DPIA.

4.23 The Council will publish and keep updated detailed fair processing information or privacy notices on its website.

Sharing Personal Data

4.23 Before sharing any personal data either internally or externally, the Council will need to consider all the legal implications of doing so. The ability to share information is subject to a number of legal constraints which go beyond the requirements of the GDPR. There are likely to be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that may affect our ability to share personal data. The Council will follow the Information Commissioner's Code of Practice on Data Sharing when deciding to share personal data.

4.24 The Council works with other external organisations to provide services. The sharing of personal data between the Council and third parties is subject to formal information sharing protocols. These set out overarching common rules adopted by the Council and its partners with whom it wishes to share data.

4.25 Details of each data sharing process are documented in information sharing agreements. A central register of all protocols and agreements will be maintained by the Data Protection Officer to ensure that transfer and sharing arrangements meet the requirements of the GDPR and the Code of Practice on Data Sharing.

4.26 All new data sharing protocols and agreements must be approved by the relevant Service Manager and the Data Protection Officer before they are used.

4.27 It is important to be aware that the data protection principles and Code of Practice apply to the sharing of information between services within the Council. For example, we should only data share where we have informed the data subject of our intention to do so.

Disclosing Personal Data

4.28 There are many instances where it will be fair and reasonable to disclose personal data with (and without) the consent of the individual. All requests for personal data and disclosures must be documented.

4.29 Information may be shared through partnership arrangements where there is a data sharing agreement in place or where the individual has authorised disclosure through a mandate.

4.30 When disclosing personal data, the Council will only disclose personal data that is necessary for the stated purpose.

4.31 The GDPR provides the following rights for individual Data Subjects**:**

(a) The right to be informed. This is usually done via privacy or fair processing notices;
(b) The right of access (Article 15). A data subject can request access to their own personal data. This is known as a Subject Access Request (SAR).
(c) The right to rectification (Article 16);
(d) The right to erasure or to be forgotten (Article 17);
(e) The right to restrict processing(Article18);
(f) The right to data portability (Article 20);
(g) The right to object (Article 21);
(h) Rights in relation to automated decision making and profiling (Article 22).

For information about SARs, and the other individual rights referred to above, see under GDPR Toolkits, Templates and Forms at the GDPR page on the Intranet.

Disclosure of Personal Data to Elected Members.

4.32 The GDPR applies to Councillors acting in their capacity as an Elected Member of the Council or a Committee of the Council.

4.33 Elected Members may request personal data in the course of their work, for example as a Committee Member, or acting on behalf of a constituent. Elected Members will only be given access to personal data when knowledge of the content of such data is necessary for them to undertake their Council responsibilities. They will be provided with access to personal information only in compliance with the provisions of the GDPR and, in particular, the Data Protection Principles, or when the relevant data subject has authorised the access in writing.

4.34 Personal Data disclosed to Elected Members will remain the property of the Council and cannot be used or disclosed for purposes other than those for which it was provided.

Disclosure of Personal Data relating to Crime, or required by Law etc

4.35 Schedule 2 to Act contains exemptions to the GDPR's transparency obligations and individual rights which permits the Council to disclose personal data for the purpose of prevention and detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of taxes or duties. Organisations making such a request must complete the Council's standard form which can be found on the GDPR page of the Intranet.

4.36 Schedule 2 also allows the Council to disclose personal data if it is required in connection with legal proceedings.

4.37 Each request shall be considered on a case by case basis and must be forwarded to the relevant Service Manager for processing and response. The Service Manager must keep records relating to any such requests and follow the Schedule 2 procedure which can be accessed from the GDPR page on the Intranet.

Unauthorised Disclosure

4.38 All Elected Members, Council staff, including Temporary staff, Contractors, Consultants and Volunteers that access and use Council information must never disclose personal data obtained in the course of their work with the Council, or access personal data without appropriate permissions. It is a criminal offence to knowingly obtain or disclose personal data without the consent of the Council as Data Controller.

4.39 In respect of employees, a breach of data protection legislation and/or the Council's related policies may be dealt with under the Council's Disciplinary Procedures. As regards Elected Members, a breach may be subject to the Council's internal complaints procedure and also to a complaint to the Standards Commission.

Training

4.40 All Employees, Contractors, Consultants and Volunteers need to be aware of their obligations under GDPR. A variety of training methods will be employed to ensure appropriate levels of awareness, understanding and knowledge.

Security

4.41 The Council will ensure that appropriate controls are in place to keep personal data secure at all times. If personal data needs to be transferred outside of the European Economic Area then the Council will comply with the conditions of transfer set out in Chapter V of the GDPR.

4.42 The Council's policies on Information Security, including ICT Acceptable Use, Home Working, and Records Management must be followed at all times. Particular care should be given to the display and transportation of personal data to ensure that unauthorised access or disclosure is not made whether by accident or design.

Reporting and Managing Data Protection Breaches

4.43 A Data Protection Breach can occur through the theft or accidental loss of personal data (for example, laptops, tablets, portable devices, and files containing personal data). They can also occur through the unauthorised use or accidental disclosure of personal data by employees, or deliberate attacks on Council systems.

4.44 All Data Protection Breaches must be reported to the Data Protection Officer in accordance with the Council's Data Protection Breach Procedure. This will allow the Council to take all the necessary steps to recover the data and limit any potential damage caused by the breach.

4.45 The Council will 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 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. A notifiable breach has to be reported to ICO without undue delay and within 72 hours of the Council becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows us to provide information in phases.

4.46 Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council must also notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the ICO**.** If the breach is sufficiently serious to warrant notification to the public, the Council must do so without undue delay. If the Council requires to notify data subjects of breach then it will also need to notify the ICO given that a higher threshold will have been met.

4.47 Failing to notify a breach to the ICO or individual data subjects when required to do so could result in the Council facing a significant fine up to 10 million Euros.

Data Processors

4.48 Contractors and Consultants will carry out work and process personal data on the Council's behalf to help deliver services. In such cases, the Council is considered to be the 'Data Controller' responsible for that personal data, and the Contractor or Consultant is the 'Data Processor' who processes the data on behalf of the Council.

4.49 Such arrangements must be governed by written agreements or contracts to ensure compliance with this policy and the data protection principles, including on-going monitoring.

4.50 The Data Protection Officer, Records Management Officer and Information Governance and Security Lead must be consulted before engaging Contractors or Consultants who process personal data.

4.51 The Data Protection Officer shall ensure that the Procurement Service maintains a list of all Council contracts where a Contractor or Consultant acts as a Data Processor.

Records Management

4.51 All personal data must be held, retained and reviewed in accordance with the Council's Records Management Policy and agreed retention schedules.

4.52 In order to ensure that the Council can demonstrate compliance with the GDPR it must document its processing activities and maintain internal records. It is therefore essential that Data Protection audits are carried out across all departments processing personal data on an annual basis in order to ensure that the Council is complying and continues to comply with the GDPR. Movement of personal data files must be tracked and recorded.

Information Asset Register

4.53 An Information Asset Register will be maintained by each Service Manager. The register identifies personal data and sensitive personal data held by the Council, and helps to evaluate and assure compliance with the Council's policies and processes, recording and highlighting risk, as appropriate. The Records Management Officer will maintain an overall Information Asset Register for the Council.

Integrated Services under the Midlothian Joint Integration Board (MJIB)

4.54 Where personal data is processed for the purpose of delivering an integrated service under the Integration Scheme of the MJIB, the Council, NHS Lothian and MJIB are all Joint Data Controllers in respect of that data processing.

4.55 There is a formal Memorandum of Understanding between the Council, NHS Lothian, and the MJIB which sets out how our Joint Data Controller status is managed and services delivered.

Implementation

5.1 The Information Management Group will approve and monitor an annual action plan for information governance development and compliance, including data protection. The plan will outline key tasks, outcomes, accountabilities and progress.

Roles and responsibilities:

Information Management Group

6.1 The Council has established an Information Management Group (IMG) whose remit includes considering and advising on personal data management issues at a strategic level across the Council and reporting to the Corporate Management Team (CMT) as appropriate. The work of the IMG underpins the Council's commitment to ensure the privacy of its customers. The IMG has delegated responsibility, through the SIRO and the CMT for the development and delivery of effective data protection governance throughout the Council.

6.2 The IMG plays an important role in ensuring the Council follows best practice in complying with the GDPR.

6.3 To support the IMG and Data Protection Officer each Division shall nominate a an appropriate Data Protection Compliance representative and allocate adequate resource

to promote and monitor data protection management practice within their Division. The Data Protection Compliance representative will attend meetings of the IMG.

Corporate Management Team

6.4 The Corporate Management Team (CMT) has overall responsibility for data protection compliance. This involves providing high-level support to ensure that each Division applies relevant information governance policies and controls.

Senior Information Risk Owner

6.5 The Head of Finance and Integrated Support Services is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the CMT with specific responsibility for information risk and mitigation, ensuring that information threats and breaches are identified, assessed and effectively managed.

Data Protection Officer

6.6 The Council is required by the GDPR to appoint a Data Protection Officer (DPO). The main tasks of the DPO are:

(a) to inform and advise the Council and its employees about their obligations to comply with the GDPR and other data protection laws;

(b) 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.

(c) to be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).

6.7 The DPO will report to the SIRO and operate independently. The DPO is not to be dismissed or penalised for performing their task. The Council shall ensure that adequate resources are provided to enable the DPO to meet their GDPR obligations.

6.8 The DPO role will sit within the Council's Legal Services section.

Directors and Heads of Service

6.9. Each Director will retain executive authority for compliance with the GDPR within their Division and each Head of Service will be responsible for ensuring that their service's information and systems comply. Each Director will be required to nominate an appropriate officer to act as Data Protection Compliance representative for their Division. Their main role will be in monitoring compliance within their Division, in passing on advice and training, in maintaining the accuracy of their Divisions input into the Council's notification, and processing subject access requests which relate to records from their Division. The Data Protection Officer will maintain an up-to-date list of these officers.

Managers

6.8 All Managers must:

6.8.1 Ensure that this Policy and any associated procedures governing the use of personal information (Corporate and Service related) are in place, understood and followed by all staff within their business areas.

6.8.2 Ensure that their staff have received data protection training (appropriate to their role), and maintain records as to when initial and refresher training has taken place;

6.8.3 Review and revise procedures if processes governing the use of personal information are subject to change within their business areas;

6.8.4 Consult the divisional Data Protection Compliance representative when there is a proposed change to the use of personal information, or when new projects are being considered;

6.8.5 Undertake Data Protection Impact Assessments in respect of new projects or new processing of personal information;

6.8.6 Consult the Data Protection Compliance representative before signing up to, or revising, and information sharing protocol or agreement;

6.8.7 Report any suspected breaches of confidentiality or information loss to the Information Data Protection Officer and follow the breach reporting procedure;

6.8.8 Identify any existing or emerging information risks relating to personal information and report to the Data Protection Officer and, if required, record on local and divisional risk registers;

6.8.9 Ensure that timely and appropriate responses are provided to SARs and other individual data subject rights;

6.8.10 Ensure that there are appropriate procedures and measures in place to protect personal data, particularly when that information (hardcopy and electronic) is removed from Council premises;

6.8.11 Undertake annual data protection compliance self-assessments to ensure ongoing compliance with this policy; and

6.8.12 Provide a statement of assurance to evidence data protection compliance; and

6.8.13 Inform their Data Protection Compliance representative (when requested) of activities containing personal data (paper or electronic) to facilitate the Council's record keeping obligations.

Staff

6.9 All staff have responsibility for data protection compliance and must:

6.9.1 Read, understand and follow this Policy and any associated procedures that relate to the use and handling of personal information in the course of their work;

6.9.2 Undertake appropriate data protection training (including annual refresher training) and ensure they have a clear understanding of their responsibilities in using and handling personal information;

6.9.3 Identify and report any risks to personal information to their line manager;

6.9.4 Identify and report suspected breaches of confidentiality or compromised personal data to their Line Manager;

6.9.5 Identify and forward any SARs and other individual data subject rights requests to the divisional Data Protection Compliance representative to ensure that requests can be processed in accordance with statutory timescales; and

6.9.6 Assist customers in understanding their information rights and the Council's responsibilities in relation to data protection.

Related documents/

Related documents

Policy

7.1 ICT Acceptable Use Policy

7.2 Information Security Policies and Procedures

7.3 Record Management Policy

Guidance and Procedures

7.4 ICO Guide to GDPR

7.5 GDPR –Toolkits, Templates and Forms

7.6 GDPR –Privacy Notices

7.7 GDPR – Information Sharing

7.8 Information Security Training

7.9 Employee Code of Conduct

Legislation

7.10 General Data Protection Regulation

7.11 Data Protection Act 2018

Sustainability impact

8.1 There are no sustainability issues arising from this Policy.

Risk Assessment

9.1 Failure to comply with any requirement of the GDPR could result in enforcement action by the Information Commissioner. The ICO has a wide range of enforcement powers which include imposing fines of up to 20 million Euros in the most serious of cases.

9.2 Individuals may take action against the Council through the Court for any misuse of their personal data which may result in the Council having to pay damages.

9.3 Failure to respond to any of the time critical response requirements in relation to information rights for individuals will result in a breach of the GDPR.

9.4 Mishandling of personal information will have serious reputational impact to the Council.

9.5 Mishandling of personal information may have serious implication to one, or more, individuals.

9.6 Personal information that is inaccurate or out of date may result in a serious negative impact on one or more individuals.

Review

10.1 This Policy will be reviewed annually or more quickly if required by significant changes in Legislation, Regulation or Business Practice. It will be reviewed by the Information Management Group and presented to the CMT as necessary.

APPENDIX

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

Processing of special categories of personal data (data concerning race, political opinions, health, etc) is generally prohibited unless explicit consent is obtained.

The GDPR does however allow processing to take place in certain circumstances without consent and enables UK law to stipulate the conditions and safeguards around this processing in certain cases. The processing of special categories of data and criminal conviction and offences data must be undertaken with adequate and appropriate safeguards to ensure the absolute protection of individuals' most sensitive personal data. The Act replicates the provisions in the Data Protection Act 1998 that allow the processing of this sort of data. Importantly, the Act provides equivalent provision as far as possible to allow for continued processing for 'substantial public interest' purposes, to ensure that organisations, such as the Council, are able to continue lawfully processing data whilst also achieving a balance between individuals' rights.

Lawfulness of processing conditions

Article	Condition
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.**

The GDPR allows member states to introduce more specific provisions in relation to Articles 6(1) (c) and (e). These provisions are particularly relevant to public authorities and highly regulated sectors. The Act provides that the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for—
(a) the administration of justice,
(b) the exercise of a function of either House of Parliament,
(c) the exercise of a function conferred on a person by an enactment, or
(d) the exercise of a function of the Crown, a Minister of the Crown or a government department.

Conditions for special categories of data

Article	**Condition**
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).

The GDPR allows member states to introduce more specific provisions in relation to Articles 9 (2) (b) (g) (h) (i) and (j). The processing meets the requirement in point (b), (h), (i) or (j) if it meets a condition in Part 1 of Schedule 1 to the Act and meets the requirement in point (g) if it meets a condition in Part 2 of Schedule 1 to the Act.

Point (g) the 'substantial public interest' condition is of relevance to Council processing and is met if the processing—
(a) is necessary for a purpose listed in sub-paragraph (2) below, and
(b) is necessary for reasons of substantial public interest.
(2) Those purposes are—
(a) the administration of justice;
(b) the exercise of a function of either House of Parliament;
(c) the exercise of a function conferred on a person by an enactment;

(d) the exercise of a function of the Crown, a Minister of the Crown or a Government Department**.**

Processing of Personal Data relating to Criminal Convictions and Offences

Processing of Personal Data relating to criminal convictions and offences or related security measures meets the requirement in Article 10 of the GDPR if it meets a condition in Part 1, 2 or 3 of Schedule 1 to the Act.