Managing Personal Data Policy

Implementation date: 4 October 2016

Control schedule

Approved by	Corporate Policy and Strategy Committee
Approval date	4 October 2016
Senior Responsible Officer	Kevin Wilbraham, Information Governance Manager
Author	Sarah Hughes-Jones, Information Compliance Manager
Scheduled for review	October 2017

Version control

Version	Date	Author	Comment
0.1	06.07.2016	Sarah Hughes-Jones	Draft policy
0.2	21.08.2016	Kevin Wilbraham	Minor comments incorporated
0.3	22.08.2016	Kevin Wilbraham	Further comments incorporated
0.4	26.08.2016	Kevin Wilbraham	Reformatting and updates around guidance
1.0	04.10.2016	Kevin Wilbraham	Approved by CP&S
1.1	02.05.2018	Kevin Wilbraham	Revised to reflect legislative changes

Committee decisions affecting this policy

Date	Committee	Link to report	Link to minute
30-09-2014	Corporate Policy & Strategy	Information_Governance_Policies	Minute
04-10-2016	Corporate Policy & Strategy	Information_Governance_Policies	Minute

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Managing Personal Data Policy

Policy statement

1.1 This policy sets out and formalises the City of Edinburgh Council's (the Council) approach to managing personal data in accordance with the requirements of the EU General Data Protection Regulation (GDPR), and in preparation for the new Data Protection Act 2018.

1.2 It outlines the Council's commitment to the principles enshrined within GDPR, and the need to balance the rights of individuals with the functions and operational requirements of the Council.

Scope

2.1 This policy applies to:

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

2.1.2 All Council staff, including temporary staff, contractors, consultants and volunteers that access and use Council information; and

2.1.3 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 –** a legal person or organisation who determines the purposes for which, and manner in which, personal information is to be processed. This may be an individual or an organisation. Data Controllers can process personal data jointly with other data controllers for specified purposes. The City of Edinburgh 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. The Council retains full responsibility for the actions of the data processor in relation to the personal data.

3.3 **Data Protection Impact Assessment (DPIA)**: an assessment tool to evidence compliance against the data protection principles. It is Council policy for DPIAs to be completed on all occasions when new processes handling personal data are introduced or changed. It is mandatory, under law, for organisations to complete a DPIA for all high-risk processing.

3.4 **Data Protection Act 1998** – gives effect in the UK law to the EC Directive 95/46/EC and came into force on 1 March 2000 repealing the Data Protection Act 1984. The Data Protection Act 1998, together with a number of Statutory Instruments, requires data controllers to comply with the legislation governing how personal data is used for statutory and business purposes. Amendments have also been created by other legislation such as the Freedom of Information Act 2000. It gives rights to individuals in relation to how organisations can use their personal data.

3.5 **Data Protection Act 2018** – The UK Government published a new Data Protection Bill in September 2017. It sets out new standards for protecting personal data (in accordance with GDPR) and preserves certain exemptions available under the current Data Protection Act 1998. It also transposes into domestic legislation the EU Law Enforcement Directive. The new Bill will result in a new Data Protection Act replacing the current Data Protection Act (1998) and will add clarity on how the UK will apply statutory controls to areas of the GDPR where Member States have been given some flexibility. As and when the UK leaves the EU, the new Data Protection Act would replace the GDPR.

3.6 **Data Protection Officer** (DPO) - is responsible for monitoring the Council's compliance with data protection principles, and providing advice to Senior Management on data protection issues. They are also the key contact between the Council and the ICO. The Council's DPO is the Information Governance Manager.

3.7 **Data Subject** – the living individual to whom the data relates.

3.8 **Edinburgh Integrated Joint Board (EIJB)** – 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 EIJB constituted under the Public Bodies (Joint Working) (Scotland) Act 2014.

3.9 **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 Data Protection Act 1998. 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.

3.10 **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).

3.11 **General Data Protection Regulation (GDPR)** – is the new data protection regulation which is force from 25 May 2018. It builds upon, and strengthens, the compliance regime provided by the Data Protection Act 1998.

3.12 **Information Commissioner -** is the independent regulator responsible for ensuring all organisations comply with the Data Protection Act. Organisations are required to notify the ICO of how they process personal data and if they breach the Act. The Commissioner has been granted enforcement powers regarding non-compliance, these include the ability to issue information and enforcement notices, impose large fines, and bring a criminal case against an organisation. Further information about data protection is available on the ICO website at www.ico.org.uk.

3.13 **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.

3.14 **Information Security** – ensures that Council information is not compromised by unauthorised access, modification, disclosure or loss.

3.15 **Information (or data) Sharing** – ensures that Council information is shared in a compliant, controlled and transparent manner.

3.16 **Notification** – is the process by which organisations notify the Information Commissioner about the categories of personal information it processes and the purposes the personal information is being processed for. The Information Commissioner uses this information to maintain a Register of Data Controllers which it publishes on its website.

3.17 **Organisational controls** - are measures that are taken to protect personal data that the Council processes. These can data protection training, documented procedures, physical security measures, and governance controls such as information sharing agreements and contract clauses.

3.18 **Personal data (or information)** – is information about a living individual who can be identified from that information or from additional information held, or obtained, by the Council. Examples of personal data are contained in paper files, electronic records and visual and audio recordings.

3.19 **Processing** – is all actions relating to personal data. Gathering, recording, analysing, amending, using, sharing, disclosing, storing and destroying personal data are all covered by this definition.

3.20 **Privacy notice** - this is information provided to data subjects to inform them about why we need their personal data and what we will do with it.

3.21 **Record of processing** - is a register of all the activities undertaken by the Council which process personal data. The Council's Register of Processing is managed by the IGU and is available on the Council's website.

3.22 **Special category data** - particular types of personal data which are considered to be more sensitive e.g. information about health, religious beliefs, political opinions, trade union membership, sexual orientation, ethnicity, and biometric or genetic data.

3.23 **Subject Access Request (SAR) -** the right granted to an individual by the Data Protection Act 1998 to request a copy of personal information held about them.

3.24 **Technical controls** - are specifically technical measures which protect personal data held or processed electronically. These are particularly relevant when new systems are being introduced and may include access controls, vulnerability testing, and encryption arrangements.

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 that govern how organisations manage personal data. They are:

4.2.1 Personal data is processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').

4.2.2 Personal data is obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

4.2.3 Personal data processed is adequate, relevant and limited to what is necessary ('data minimisation').

4.2.4 Personal data is accurate and, where necessary, kept up to date ('accuracy').

4.2.5 Personal data is not to be kept longer than is necessary for that purpose ('storage limitation').

4.2.6 Appropriate technical and organisational measures shall be taken to prevent unauthorised or unlawful processing, loss, damage or destruction ('integrity and confidentiality')

Designing or revising processes which collect and use personal data

4.3 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.

4.4 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.

4.5 Specifically, a DPIA must be carried out by service areas when:

4.5.1 Council projects or programmes are undertaken

4.5.2 Service activities commence, end or are significantly adjusted; and/or

4.5.3 New ICT arrangements are put in place which use and process personal data with a potential impact on the privacy of individuals

4.6 Completed DPIAs will be registered with the Information Governance Unit.

Transparency and data processing

4.7 When collecting personal data, the Council will inform data subjects about why their personal data is needed and how it will be used, shared and stored. This is called a Privacy Notice. The Council will make privacy information available in several ways - on the Council's website, by an audio message, through a video link or form part of a leaflet.

4.8 Appropriate privacy information will be provided at the time personal data is collected from data subjects, or when the Council first contacts the data subject in relation to the personal data they have provided.

4.9 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.

4.10 Fair processing information must be approved by the Information Governance Unit and documented within the relevant DPIA.

4.11 As part of its legal requirements, the Council maintains a 'Record of Processing' that sets out the functions and activities that involve the processing of personal data. Additions or changes to the Record of Processing must be approved by the Information Governance Unit.

Sharing Personal Data with other organisations

4.12 The Council works with other 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.

4.13 Details of each data sharing process are documented in information sharing agreements. A central register of all protocols and agreements is maintained by the Information Governance Unit to ensure that transfer and sharing arrangements meet the requirements of the GDPR, and the Information Commissioner's guidance on information sharing.

Disclosing Personal Data

4.14 There are many instances where it will be fair and reasonable to disclose personal data. All requests for personal data and disclosures must be documented.

4.15 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.

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

4.17 Data subjects can request access to their own personal data; this is known as a Subject Access Request (SAR). For information about SARs, and other rights of access to information, see the Information Rights Policy.

Disclosure of personal data to Elected Members.

4.18 Elected members may request personal data during their work, for example as a committee member, or acting on behalf of a constituent. Elected Members will be given access to the personal data they need to carry out their duties, in line with data protection legislation and the Member/Officer Protocol.

Disclosure of personal data relating to crime, or required by law

4.19 Data protection legislation allows the Council to consider disclosing 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.

4.20 The legislation also allows the Council to disclose personal data if it is required for legal proceedings.

4.21 Each request is considered on a case by case basis and must be forwarded to the Information Governance Unit for processing and response.

Unauthorised Disclosure

4.22 Employees (and others covered by this policy) 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 data controller (the City of Edinburgh Council).

Training

4.23 All employees, contractors, consultants and volunteers need to be aware of their obligations under the Act. A variety of training methods will be employed to and are available to ensure appropriate levels of awareness, understanding and knowledge.

Security

4.24 The Council will ensure that appropriate controls are in place to keep personal data secure at all times. This will include ensuring appropriate arrangements are made should personal data need to be transferred outside of the European Economic Area.

4.25 The Council's policies on Information Security, including ICT Acceptable Use, Home Working, and the Guidance Note on Protecting Personal Data, 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

4.26 A Data Protection Breach can occur through the theft or accidental loss of personal data (for example, laptops, tablets, portable devices, 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. Non-compliance with any of the data protection principles is a breach.

4.27 All Data Protection Breaches must be reported to the Information Governance Unit 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.

Data Processors

4.28 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.

4.29 Such arrangements must be governed by contract to ensure compliance with this policy and the legal requirements under GDPR, regardless of contract value.

Records Management

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

Registration

4.31 As a data controller, the Council is required to register with the Information Commissioner.

4.32 Elected Members are data controllers in relation to their constituency work and must be registered with the Information Commissioner.

4.33 The Information Governance Unit is responsible for co-ordinating the renewal of the Council's and Elected Members' registration each year.

4.34 All registered data controllers are recorded on the UK Data Protection Register which is available on the Commissioner's website.

Information Asset Register

4.35 An Information Asset Register is maintained by the Information Governance Unit. The register identifies personal data and special category data (sensitive personal data) held by the Council, and helps to evaluate and assure compliance with the Council's information governance policies and processes, recording and highlighting risk as appropriate.

Integrated Services under the Edinburgh Integrated Joint Board (EIJB)

4.36 Where personal data is processed for the purpose of delivering an integrated service under the Integration Scheme of the Edinburgh Integration Joint Board (EIJB), the Council, NHS Lothian and EIJB are all Joint Data Controllers in respect of that data processing.

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

Implementation

5.1 The Information Council 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

6.1 The Information Governance Policy provides a detailed explanation concerning overall roles and responsibilities around information governance. This section provides a summary of those responsibilities, but also outlines specific responsibilities in relation to compliance with the GDPR.

Elected Members

6.2 Elected members are covered by the Council's notification when carrying out official duties for the Council but they are required, by law, to hold a separate registration for their constituency work.

Council Leadership Team

6.3 The Council Leadership Team has overall responsibility for information governance. This involves providing high-level support to ensure that each directorate applies relevant information governance policies and controls, including compliance with the GDPR. Responsibility also extends to personal data that is processed by third parties within their respective areas of responsibility.

Senior Information Risk Owner

6.4 The Head of Strategy and Insight is the Council's Senior Information Risk Owner (SIRO). The SIRO has delegated authority through the Council Leadership Team with specific responsibility for information risk and mitigation, ensuring that

information threats and breaches are identified, assessed and effectively managed.

Data Protection Officer

6.5 The Council's Information Governance Manager is the Council's Data Protection Officer (DPO). The DPO is responsible for ensuring that the organisation is compliant with GDPR and the future Data Protection Act 2018. The DPO must also be able to act independently, be adequately resourced, and be able to report directly to senior management to raise concerns.

Information Governance Unit

6.6 The Information Governance Unit is part of Strategy and Insight with responsibility for the day to day operation and delivery of information governance within the Council. In relation to data protection it will support the DPO and do the following:

6.6.1 Act as the first point of contact for all data protection issues affecting the Council;

6.6.2 Provide guidance and advice on data protection issues for Council services;

6.6.3 Renew and amend the Council's data protection registration to the ICO

6.6.4 Co-ordinate, process and respond to all subject access requests;

6.6.5 Oversee and quality assure all data sharing protocols and agreements between the Council and other partner agencies;

6.6.6 Record and maintain the Council's information risk register, including risks relating to data protection and associated information governance activities;

6.6.7 Create, maintain and renew training modules and toolkits as appropriate;

6.6.8 Provide data protection training and raise awareness through regular communications

6.6.9 Maintain and report on key performance indicators for information governance;

6.6.10 Lead and advise on compliance requirements where the processing of personal data is complex (e.g. multi-agency working);

6.6.11 Co-ordinate the Council's information breach procedures;

6.6.12 Carry out information governance risk assessments;

6.6.13 Maintain the Council's Record of Processing;

6.6.14 Record and maintain the Council's register of information sharing agreements; and

6.6.15 Record and maintain the Council's register of Data Protection Impact Assessments.

Managers

6.7 All managers must:

6.7.1 Ensure that this policy and any associated procedures governing the use of personal information (corporate and local) are in place, understood and followed by all staff within their business areas (including contractors and consultants).

6.7.2 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;

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

6.7.4 Consult the Information Governance Unit when there is a proposed change to the use of personal information, or when new projects are being considered;

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

6.7.6 Consult the Information Governance Unit before signing up to, or revising, and information sharing protocol or agreement;

6.7.7 Report any suspected breaches of confidentiality or information loss to the Information Governance Unit and follow the breach reporting procedure;

6.7.8 Identify any existing or emerging information risks relating to personal information and report to the Information Governance Unit and, if required, record on local, divisional and directorate risk registers;

6.7.9 Ensure that personal data required to answer a subject access request is provided timeously to the Information Governance Unit;

6.7.10 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;

6.7.11 Undertake annual information governance self-assessments to ensure ongoing compliance with this policy and associate information governance activities;

6.7.12 Provide a statement of assurance to evidence information governance compliance; and

6.7.13 Inform the Information Governance Unit (when requested) of activities containing personal data (paper or electronic) to facilitate the Council's notification process with the Information Commissioner.

Staff

6.8 All staff (including contractors and consultants) have responsibility for data protection and must:

6.8.1 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;

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

6.8.3 Identify and report any risks to personal information to their line manager

6.8.4 Identify and report suspected breaches of confidentiality or compromised personal data to their line manager;

6.8.5 Identify and forward any subject access requests to the Information Governance Unit to ensure that requests can be processed in accordance with statutory timescales; and

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

Related documents

7.1 Data Quality Policy

7.2 ICT Acceptable Use Policy

7.3 Information Governance Policy

7.4 Information Rights Policy

7.5 Information Security Policy

7.6 Record Management Policy

7.7 Employee Code of Conduct

7.8 Open Data Strategy

7.9 Data Protection Breach Procedure

7.10 Data Protection Impact Assessment Guidance

7.11 Information Sharing Guidance

Equalities impact

8.1 There is no adverse impact on any group in terms of race, religion, disability, ethnic origin, sexuality or age in relation to this policy.

Sustainability impact

9.1 There are no sustainability issues arising from this policy.

Risk assessment

10.1 Failure to comply with GDPR requirements could result in enforcement action by the ICO and significant monetary penalties.

10.2 Individuals may take action against the Council through the Court for any misuse of their personal data. Depending on which Court takes the action, fines could be unlimited.

10.3 Failure to renew or amend the Council's Data Protection Registration is a criminal offence.

10.4 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 legislation.

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

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

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

Review

11.1 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 Council and presented to the Council committee annually, in line with the Council's Policy Framework.