St.Helens Council

Data Protection Policy

Version: 3.0

Date: May 2018

Version Control

Date	Version	Comments
October 2013	1.0	First finalised version
September 2015	1.1	Policy subject to full review
December 2015	1.2	Draft approved by IMG
February 2016	1.2	Union Consultation
March 2016	2.0	Approved by Executive Decision
March 2017	2.1	Annual Review
May 2018	3.0	Review for legislative changes (GDPR)

Table of Contents

1 Introduction

1.1 The Council has a legal obligation to comply with data protection legislation, which aims to protect all personal data which is collected, processed, stored and disposed of by an organisation.

1.2 Personal data is data which relates to a living individual and which allows the relevant individual to be identified either on its own or when it is combined with other personal data held.

1.3 The Council must gather and process personal information about staff and clients in order to operate effectively.

1.4 The Council, acting as the custodians of personal data, recognise their legal and moral duty to ensure that personal data is handled properly and confidentially at all times.

2 Policy Statement

2.1 This Policy document outlines how the Council delivers an effective approach to ensuring compliance with data protection legislation.

2.2 The aim of this Policy is to ensure that personal information is:

- Fairly and lawfully processed
- Processed for specific purposes
- Accurate, relevant and not excessive
- Kept accurate and up to date
- Not kept for longer than necessary
- Kept secure
- Processed in line with the data subjects (individuals) rights
- Not transferred to other countries without adequate protection

3 Scope

3.1 This Policy applies to all personal data held both on paper and by electronic means.

3.2 This Policy covers the whole lifecycle of personal data including:

- The obtaining of data
- The storage and security of the data
- The use and disclosure of the data
- The sharing of data
- The disposal and destruction of the data

3.3 This Policy applies to all Employees and third parties working for or on behalf of the Council who have access to Council information in any format, network and systems. For the purpose of this Policy the term ‘Employee’ refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

3.4 This Policy should be read in conjunction with the Data Protection Code of Practice, and other associated relevant policies, procedures and guidance as contained within the Information Management Framework.

4 Data Protection Legislation

General Data Protection Regulation Principles

4.1 The Council will maintain appropriate safeguards to ensure adherence to the six personal data principles, the data controller principle, the rights of data subjects and transferring data outside the European Union (EU).

4.2 Personal Data Principles:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subjects (lawfulness, fairness and transparency).
2. 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose (purpose limitation).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
4. 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 (accuracy).
5. 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (storage limitation).
6. 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 (integrity and confidentiality).

4.3 Data Controller Principle:

The controller shall be responsible for, and able to demonstrate compliance with the personal data principles (accountability).

Data Subject Rights

4.4 The rights of individuals (data subjects) should also be observed and St. Helens Council must ensure that these rights can be fully exercised, where appropriate, under data protection legislation. These include:

- the right to be informed (Privacy Notice);
- the right of access (to their own personal data);
- the right to rectification (inaccuracies corrected);
- the right to erasure;
- the right to restrict processing;
- the rights in relation to automated decision making and profiling;
- the right to data portability;
- the right to object.

Transferring Data Outside the EU

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

5 Data Breaches

5.1 A data breach (potential or actual) occurs where personal data may have been destroyed, lost, altered, or disclosed / accessed without authority.

5.2 Where a data breach has been identified, it must be reported internally in line with the Data and ICT Security Incident Management Policy.

6 Data Protection Impact Assessments (DPIA)

6.1 DPIAs must be completed when using new technologies in a way that is likely to result in a high risk to the rights and freedoms of individuals.

6.2 Where a DPIA is required, the Senior Information Management Officer (SIMO) must be consulted from the beginning of the process.

6.3 Where appropriate, the SIMO in consultation with the Data Protection Officer (DPO) will engage with the Information Commissioner's Office (ICO) regarding the DPIA.

7 Information Commissioner's Office (ICO)

7.1 The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

7.2 The ICO reports directly to UK Parliament.

7.3 The Council should inform the ICO of any breach which is likely to result in a risk to the rights and freedoms of individuals, within timescales.

8 Responsibilities

Data Protection Officer (DPO)

8.1 The DPO is a member of senior management who has overall responsibility for data protection in the Council, and acts in an impendent manner in line with legislation.

8.2 They are the named person on all official documentation and would be cited in any case where legal action is taken against the Council.

8.3 The DPO is responsible for gathering and disseminating information and issues relating to data protection.

8.4 The DPO is responsible for ensuring that necessary fees are paid to the ICO.

8.5 The DPO is also the key contact with the ICO.

Information Management Group (IMG)

8.6 The role of the Information Management Group (IMG) is to co-ordinate the approach to every aspect of Information Management, and not just compliance with DPA 1998.

8.7 The group is made up of Departmental Information Management Representatives who are senior managers in each Department and are responsible for a multi-disciplinary approach to the management of information throughout their Departments.

8.8 The IMG is responsible for the overarching governance and implementation of the Policy throughout the Council.

8.9 The IMG is responsible for ensuring that all Employees are fully aware of Council policy and process, and have received appropriate training.

8.10 The IMG is also responsible for the development and monitoring of the adherence to the Policy.

Senior Information Management Officer (SIMO)

8.11 The SIMO will carry out all delegated duties and tasks of the DPO, and ensure that the DPO is fully informed of any duties and tasks carried out on the DPO's behalf.

8.12 The SIMO will carry out the day to day workings of data protection compliance, and audit the provisions for the same in Departments.

8.13 The SIMO is responsible for ensuring that the Policy remains accurate and up to date.

8.14 The SIMO is responsible for co-ordinating investigations into potential data breaches, and reporting to the ICO when necessary, as per the Data and ICT Security Incident Management Policy.

8.15 The SIMO will maintain a record of processing activities.

8.16 It is also the SIMO's role to advise on all data protection matters.

Line Managers

8.17 Line Managers will have responsibility for all matters relating to data protection in their operational area and all initial queries should be referred to them.

8.18 Line Managers must ensure that service procedures document how this Policy and the Principles are to be applied in their service area (where applicable).

8.19 Line Managers are responsible for ensuring all Employees in their operational area adhere to the Policy and have undertaken all relevant training.

8.20 Line Managers must ensure that all data breaches are reported to the IT Service Desk.

8.21 Line Managers must ensure where a data breach (including potential breaches) occurs a completed Data Breach Notification Form is returned within 24 hours of becoming aware of the breach.

8.22 Line Managers must complete a DPIA when required, in consultation with the SIMO.

8.23 Concerns regarding compliance with data protection should be reported to the SIMO.

Employees

8.24 All Employees will be responsible for safeguarding the personal data in their care. This carries with it a responsibility to abide by this Policy, the Data Protection Code of Practice, and related policies, procedures and legislation.

8.25 All Employees who handle personal data must undertake all relevant training in data protection.

8.26 Queries in relation to data protection issues in the workplace should always be referred initially to Line Managers.

9 Review and Governance

9.1 The Policy will be subject to governance through the IMG, and will be formally approved by Strategic Directors Group via the Executive Decision Framework.

9.2 The Policy will be subject to at least an annual review, and where changes in legislation require, more frequent.

10 Policy Compliance

10.1 If you are found to have breached this Policy, the matter will be considered and investigated under the Council's disciplinary procedure.

10.2 Serious breaches of this Policy may constitute gross misconduct and lead to summary dismissal. Breaches, where applicable, may also result in civil action and/or criminal charges.

10.3 Under data protection legislation, legal liability for the safeguarding of personal data falls both to the organisation and individually to its employees. Prosecutions can be undertaken under the legislation.