Stevenage Borough Council's Data Protection Guide for the Public

Contents

Guidance Statement

To operate efficiently, Stevenage Borough Council must collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of government.

Stevenage Borough Council regards respect for the privacy of individuals and the lawful and careful treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and proportionately.

To this end Stevenage Borough Council is committed to protecting the rights and privacy of individuals including those rights set out in the General Data Protection Regulation and other data protection legislation.

The Council's principal aim is to ensure that all personal data processing carried out by the Council, or on its behalf, complies with the seven data protection principles and other key legislative requirements.

This Guidance explains how the Council handles individuals' information.

1. Introduction

The Council increasingly depends on computer systems and paper records (paper files) to carry out much of its normal business. In 1998, when the previous Data Protection Act 1998 was enacted by Parliament, the internet was in its infancy, social media and smart telephones had not been invented and the way we shared information was very different.

The GDPR and Data Protection Act 2018 protects the rights of individuals in these new circumstances. This guidance sets out how the Council will protect the rights of individuals and comply with the law.

To comply with the current legislation, all employees, elected members, consultants, volunteers, contractors and other agents of the Council who use its computer facilities or paper files to hold and process personal information are expected to follow this guidance

2. Definitions

2.1. Personal Data

This is data which relates to a living individual ("data subject") who can be identified:

- From the data.
- From the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

This includes the name, address, telephone number, national insurance number as well as any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2.2. Special Category Data

This is personal data considered to be of a sensitive nature, consisting of information as to any of the following:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex life.
- Sexual orientation.

Special category personal data is subject to much stricter conditions of processing.

2.3. **Record**

A record is recorded information, in any form, including data in systems created, received and maintained by the Council and kept as evidence of such activity.

2.4. **Format**

A record can be in any format including (but not limited to) paper files, e-mail, audio/visual, electronic documents, systems data, databases, digital images and photographs.

2.5. **Processing**

The definition of processing covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.

2.6. **Data Controller**

A Data Controller is a person or organisation who decides how any personal information can be held and processed, and for what purposes. Stevenage Borough Council is a Data Controller.

2.7. **Data Processor**

This role is carried out by any person other than a Council employee (for example, contractors and agents) who process personal information on behalf of the Council.

2.8. **Data Protection Laws**

These are laws that govern the way organisations use individuals' personal information, which are the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

3. Roles and Responsibilities

3.1. Information Asset Owners

The Information Asset Owners (IAOs) are the Assistant Directors for the Council's service units Their role is to understand what information is held by their service, what is added and what is removed, how information is moved, and who has access and why.

Through their managers, they help ensure that written procedures are in place and followed relating to how their teams handle information, that risks are assessed, mitigated and processes are documented. IAOs will appoint Information Asset Administrators (IAAs) to provide assist them in completion of such tasks

4.2. Data Protection Officer

The role of the Data Protection Officer (DPO) is to:

- Inform and advise the Council and its employees about their obligations to comply with the General Data Protection Regulation and other data protection laws.
- Monitor compliance with the General Data Protection Regulation and other data protection laws, including the assignment of responsibilities, awareness raising, and training of staff involved in the processing operations and related audits.
- Provide advice about data protection impact assessments and monitor their performance;
- Co-operate with the supervisory authority (the Information Commissioner's Office).
- Act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

The Council's DPO is the Records & Information Governance Manager.

4.3. Information Asset Administrators (IAAs)

Each Assistant Director has nominated one or more Information Asset Administrator(s) to the Council's Information Corporate Governance Group. They are responsible for providing routine advice on data protection and information governance issues to their respective services.

4.4. Records & Information Governance Manager

The Records & Information Governance Manager is responsible for developing, delivering and maintaining a comprehensive information governance framework for the Council. He/she will help ensure compliance with legislative frameworks governing the access to, retention, sharing and disposal of information.

The Records & Information Governance Manager is responsible for reporting all personal information held by the Council to the Information Commissioner.

4.5. Services, Security & Standards Manager

The Services, Security & Standards Manager is responsible for assisting the Council maintaining the Council's security Guidance and procedures to reflect changing local and national requirements.

The Services, Security & Standards Manager will support service areas on achieving best practice and compliance with security requirements.

4.6. Archivist

The Council's Facilities and Compliance Manager will ensure proper procedures are carried out in relation to the transfer of records to the archive and their subsequent storage and access.

4.7. Individual Members of Staff and Elected Members

Individual members of staff and elected members are responsible for protecting personal information held or processed on computer, or held in paper records, within their care.

4.8. Corporate Information Governance Group

The Council's Information Corporate Information Governance Group (CIGG), among its various functions in relation to information management, assists the Council in its compliance with data protection and other information legislation. The members of the CIGG are the Data Protection Officer, the Records &Information Governance Manager, the Services, Security & Standards Manager, the Archivist and the Information Asset Administrators. The CIGG is chaired by the Records & Information Governance Manager.

5. Lawful Bases for Processing Personal Information

The lawful bases for processing are set out in the Data Protection Laws. At least one of these must apply whenever the Council processes personal information:

a) **Consent**: the individual has given clear consent for the Council to process his/her personal data for a specific purpose.

b) **Contract**: the processing is necessary for a contract that the Council has with the individual, or because the individual has asked the Council to take specific steps before entering into a contract.

c) **Legal obligation**: the processing is necessary for the Council to comply with the law (not including any contractual obligations).

d) **Vital interests**: the processing is necessary to protect someone's life.

e) **Public interest**: the processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council.

f) **Legitimate interests**: the processing is necessary for the purposes of legitimate interests pursued by the Council or a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. However, this basis is not available to processing carried out by the Council in

the performance of its official tasks; it can only apply to the Council when it is fulfilling a different role.

All Council services must ensure they have a lawful basis to process individuals' information, which is detailed in the Council's Privacy Guidance.

6. Rights of Individuals

The Data Protection Laws provides individuals with the following rights regarding their personal information:

- The right to be informed about how their information will be used.
- The right of access to their personal information.
- The right to rectification, which is the right to require the Council to correct any inaccuracies.
- The right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information.
- The right to request that the processing of their information is restricted.
- The right to data portability.
- The right to object to the Council processing of their personal information.
- Rights in relation to automated decision making and profiling.

The Council has published detailed information for the public that set out what these rights are and how they can be exercised, available in our guide – Subject Access & Information Rights Leaflet & Form

7. The Data Protection Principles

The General Data Protection Regulation (GDPR) sets out seven principles for the processing of personal information which are legally binding on the Council. They are

a. Lawfulness, Fairness & Transparency Principle: Information must be processed lawfully, fairly and in a transparent manner in relation to the data subject "

b. Purpose Limitation Principle: Information must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

c. Data Minimisation Principle: Information must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d. Accuracy Principle: Information must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

e. Storage Limitation Principle: Information must be 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 Data Protection Laws in order to safeguard the rights and freedoms of the data subject.

f. **Security, Integrity & Confidentiality Principle:** Information must be 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.

g. **Accountability Principle:** This is a new principle under the GDPR, which makes the Council responsible for demonstrating compliance with the GDPR requirements.

8. Notifying the Information Commissioner

The Council must advise the Information Commissioner's Office (ICO) that it holds personal information about individuals. The Council is registered with the ICO, with registration number Z631608X.

9. Processing Personal Information

The Council will hold and process personal information only to support those activities it is legally entitled to carry out.

The Council may on occasion share personal information with other organisations. In doing so, the Council will comply with Data Protection Laws.

The Council will provide details to individuals about how it handles their personal information, the purpose for which the information will be held or processed and who the information may be shared with.

10. Training

All staff will be provided with training data protection law and practice as soon as reasonably practicable after starting to work for the Council. All staff have a confidentiality clause in their contracts of service. They also follow an Acceptable Use Policy for using the Council's systems and equipment.

Staff who work on computer systems that hold or process personal information, or who use the information associated with those systems, will receive relevant training. If written procedures for using such systems are not yet in place, staff will be trained in legitimate ways of finding and providing information and told which information must not be recorded.

Any new Information Asset Administrators will be trained in data protection relating to their information handling activities for their business area.

Managers may wish to request in-depth training for their staff, particularly if they are dealing with Special Category Data. In these circumstances they should contact the Information & Records Governance Manager in the first instance to enable appropriate arrangements to be made.

Additional refresher training and specific areas of data protection law will be available for service areas who routinely deal with more sensitive personal and/or confidential information.

Elected Members will be provided with training in data protection law and practice as soon as reasonably practicable after they are elected.

11. Information Security

The Council's approach to Information Security will be set out in its Information Security Policies.

12. Complaints

Any complaints received by, or on behalf of, a member of the public containing allegations of inappropriate disclosure of information will be dealt with in the normal way through the Council's Complaints Handling Procedure in the first instance.

If an individual does not feel that the Council is treating their data appropriately or has not answered their complaint, in the first instance they can raise any their concerns with the Council's Data Protection Officer, and if still dissatisfied with the Council's decisions, can contact the Information Commissioner.

13. Breaches of Security

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Despite the security measures taken to protect personal data held by the Council, a breach can happen.

If any security incident occurs the IT services and Data Protection Officer must immediately be informed to enable a Breach Management Plan to be put in place.

More information on breach management can be found on Information Commissioner's Office's website.

14. Monitoring and Reporting

This guidance will be reviewed annually by the Records & Information Governance Manager.

Proposed changes to information governance policies or procedures will be considered by the Records & Information Governance Manager in the first instance.

15. Related Policies and Procedures

Stevenage Borough Council Records Retention Schedule
Stevenage Borough Council Personal Information – Subject Access & Information Rights Leaflet & Form
Stevenage Borough Council Data Protection Guidance for the Public

16. Further Information and Guidance

Contact: Records & Information Governance Manager

Telephone: 01438 24 2224

Further information is also available from the Information Commissioner's website.

Document control Sheet

Review/Approval History

Date	Name	Position	Version Approved
May 2018	Dumi Williams	Records & information Governance Manager	V1.0 May 2018

Change Record Table

Date	Author	Version	Status	Reason

Status Description

Final – The document is complete and is not expected to change significantly. All changes will be listed in the change record table.