Welwyn Hatfield Borough Council

Data Protection Policy

Report Control Information

Effective Date: 25 May 2018 Author: Richard Baker

REVISION	DATE	REVISION DESCRIPTION
1	December 2017	Internal Draft

1 Introduction

1.1 Welwyn Hatfield Borough Council (the Council) collects and processes personal data in performing its statutory and discretionary functions. The General Data Protection Regulations (GDPR) set out legal obligations the Council must adhere to when processing personal data. The six key principles of GDPR are:

- Personal information must be processed fairly, lawfully and in a transparent manner
- Personal information will be collected for specified, explicit and legitimate purposes
- Personal information must be adequate, relevant and limited to what is necessary
- Personal information must be accurate and where necessary kept up to date
- Personal information must be kept for no longer than is necessary
- Personal information must be processed in a manner which ensures appropriate security of personal data.

1.2 This policy provides the framework which governs how the Council complies with its obligations under the GDPR. It applies to all employees, Councillors, volunteers, service providers, contractors, partner organisations, or any other third party data is shared with.

2 Awareness

2.1 In order for the Council to ensure employees and Councillors (see appendix C) are aware of their responsibilities the under GDPR, it will:

- approve and maintain a Data Protection Policy (this document), and make this readily available to any person including employees and Councillors;
- ensure that all staff who can access, or are responsible for processing personal data, are fully trained and aware of their responsibilities under the GDPR and other relevant policies;
- ensure regular review and update of e-learning available to employees;
- ensure training is made available to Councillors;
- produce and maintain guidance notes and procedures, ensuring these are readily available to staff and Councillors.

3 Processing and retention of personal and sensitive data

3.1 The Council will only process personal data where it has a legitimate business need to do so, and at least one of the following conditions are met:

- it is required under a legal obligation to which it is party;
- the individual has given their express consent;
- it is necessary in the protection to the vital interests of the individual or another person;
- it is necessary for the performance of a contract with the individual;
- it is necessary for a task carried out in the public interest or in the exercise of official duties.

3.2 The Council will identify the minimum amount of information required in performing its activities, and gain explicit consent, as required, when collecting sensitive personal data.

3.3 Personal data will:

- be anonymised when not required for business need;
- be retained and destroyed in line with the Council's Data Retention Guidelines;
- be accurate and up to date, with notifications of inaccuracy being investigated and corrected swiftly;
- not be held for longer than it considered reasonable for business need.

3.4 The Council's Data Retention Policy and Guidelines will:

- identify the categories of data held by the Council;
- clearly state the reasons for holding the data;
- identify how long data is held for;
- detail how the council manages disposal of data
- be subject of regular review.

3.5 Data will only be destroyed in line with the Council's data retention guidelines, or if individuals exercise their rights to be forgotten.

3.6 The Council will ensure, where appropriate, that it is able to restore the availability of, and access to data in a timely manner in the event of a physical or technical incident.

3.7 The Council will maintain an information assets register, which details the software used to process personal data.

3.8 The Council will maintain records of explicit consent and how it was maintained.

4 Security and Control Measures

4.1 In order to protect the personal information held and processed, the council will:

- ensure its use of technology is compliant with the Public Service Network Compliance (PSN);
- ensure the regular review, update and compliance with IT policies;
- ensure all electronically stored personal data is password protected or encrypted;
- ensure confidential data is secured and not left in view of those not processing the data;
- only use the blind carbon copy (BCC) in emails when sending group emails to external individuals;
- ensure documents containing personal data are not removed from site;
- not store data sent from a website (cookies);
- delete web browsing history of staff after six months;
- undertake data protection audits for each Head of Service Area, which will be logged with the Data Protection Officer;
- comply with its separate policy on patient identifiable information;
- not transfer personal information to another company or country that cannot protect the information to the same levels set out under the GDPR;
- not make publicly available or share protectively marked documents externally;
- mark emails with confidential protective marking where they contain personal or sensitive information.

5 Sharing of Data

5.1 To ensure that personal information is protected when sharing with third parties, the council will:

- ensure formal data sharing agreements are in place before data is shared;
- maintain a register of data sharing arrangements;
- only share personal data electronically that is password protected or encrypted;
- ensure adequate contractual provisions are contained within legal agreements in relation to data protection;
- where appropriate, seek to ensure that it is indemnified against any claims, proceedings, actions or payments of compensation or damages without limitation;
- arrange data protection audits of data held by third parties where appropriate.

5.2 The sub-contracting of work involving the processing of personal data, will not be allowed without:

- written confirmation from the Council;
- the same contractual obligations being imposed on the subcontractor;
- a formal data sharing agreement being in place prior to the sharing of data.

5.3 Any breach of the GDPR will be deemed as being a breach of contract.

6 Rights of individuals

6.1 The Council will only process personal information in line with the data subjects' rights. Data subjects have the following rights:

- The right to be forgotten;
- The right to be informed;
- The right to object;
- The right to make a subject access request;
- The right to object to decisions being made on them solely by a computer;
- The right to object to profiling.

6.2 To ensure individuals are aware of their rights the Council will:

- publish a privacy statement on its website;
- publish individuals' rights on our website and how they can exercise their rights;
- maintain internal procedures on the processing of individuals exercising their rights;
- inform individuals of their right object;
- review decisions generated by a computer if an individual exercises their right to object to decisions being made on them solely by a computer;
- cease to process data for profiling if an individual exercises their right to object to profiling.

6.3 The Council will ensure that the identity of an individual is confirmed before processing any exercise of individual rights.

6.4 To ensure that the Council meets its requirements in fulfilling an individual's rights, unless there are legitimate reasons which override the rights or freedoms of an individual, it will:

- stop processing data when an individual exercises their right to object;
- erase data when an individual exercises their right to be forgotten;
- inform individuals of how it is processing their data;
- provide individuals with the information the Council holds on them.

6.5 The Council will only charge a fee of £25 per hour, increasing annually each financial year by the RPI as at January prior to the start of the financial year, for access requests deemed to be unfounded or excessive. The Council will not charge a fee for subject access requests in other circumstances.

6.6 A register of subject access requests will be maintained, including the date received, the name and address of the subject, brief details of the request, and the date the subject was responded to.

7 Data Protection Breaches

7.1 The Council takes the protection of data seriously, and will always ensure it has processes and controls in place to protect data. A data breach involves any data which is lost, stolen, unlawfully accessed, unlawfully disclosed, accidentally or deliberately deleted. In the event of a breach the Council will:

- maintain a procedure for dealing with data breaches and where exemptions are in place reporting of a data breach;
- ensure the Data Protection Officer is immediately informed of any breach or suspected breach;
- inform the Information Commissioner's Office (ICO) of a breach without undue delay, and in any event, no later than 72 hours after becoming aware of the breach;
- communicate with affected data subjects without undue delay if deemed to result in a high risk to the freedoms and rights of the data subjects.

7.2 The Council will take appropriate action under the Council's conduct procedure for employees, or through contractual arrangements with third parties where the breach is a result of non-compliance with Council policies.

8 Privacy Impact Assessments

8.1 The Council will undertake a risk based assessment, known as a Privacy Impact Assessment (PIA), of any all new and existing projects and supporting IT systems.

8.2 The Council will maintain a template for Privacy Impact Assessments which will be made readily available to employees.

8.3 The Council will maintain a central register of all PIAs undertaken.

8.4 Areas where PIAs will be required includes, but is not limited to:

- implementation or upgrades of IT systems;
- new or amendments to data sharing arrangements;
- using existing data for new or alternative uses to that from its original purpose;
- new surveillance systems;
- consolidation of data held in separate parts of the organisation;
- changes to legislation, policies or strategies which may affect privacy through collection or use of information;
- new websites or mobile applications capturing personal data;
- development of online forms and interfaces with back office systems.

9 Exemptions

9.1 Only in very specific circumstances can personal data be disclosed to third parties without the consent of the data subject. The Council will only disclose personal information without the consent of the data subject where it is necessary for:

- safeguarding national security;
- preventing or detecting any crime, or the apprehension or prosecution or offenders;
- assessing or collecting any taxes, revenues or duties;
- discharging or regulatory functions, including the health, safety and welfare of people at work;
- protecting the vital interests of the individual or another individual, usually in a life or death situation.

9.2 In an emergency situation the Council will consider the risks and potential harm that may arise if it does not share the information, and any decisions to disclose data will be formally recorded and sent to the Data Protection Officer.

Appendix A - Roles and Responsibilities

Cabinet

- Approval of the policy framework (this document) within which data protection is governed by Welwyn Hatfield Borough Council.

Head of Paid Service (Chief Executive)

- Formally designate/appoint a Data Protection Officer.

Executive Board

- Ensure the importance of data protection is culturally embedded into the Council.
- Allow unfettered access to the Data Protection Officer to raise or report on any matters.
- Receive update reports, as required, from the Data Protection Officer in order to oversee compliance with the GDPR and Data Protection Policy.

Heads of Service

- Ensure that annual data audits are conducted for their services.
- Ensure data sharing arrangements and contractual provisions are in place prior to sharing data with third-parties, to provide third parties with a clear understanding of their responsibilities.
- Ensure that through the services managed, and associated forms and processes, individuals are aware of their rights under the GDPR.
- Ensure data collected, retained, processed, shared and destroyed by services/employees is done so in line with the relevant policies.
- Ensure their services have the processes in place for explicit consent to be requested and recorded where required.

Employees Comply with the data protection and other associated Council policies and guidance (such as the Data Retention and IT policies)

- Act with due diligence with regards to the GDPR. If in any doubt, at any time, guidance should be sought from the Council's Data Protection Officer.
- Report data breaches immediately to the Data Protection Officer and co-operate with the Data Protection Officer regarding the data breach reporting process.
- Proactively identify areas of risk, and make suggestions on how compliance, security, and the protection of information can be enhanced and improved.

Client Support Services Manager

- Maintenance of the Councils IT Policies, procedures and guidance

Principal Governance Officer

- Maintenance of the Council's Data Retention Policy and Guidelines.

Data Protection Officer (DPO)

- Ensures that the Council's processing operations adequately safeguard personal data, in line with legal requirements.
- To have unfettered access to the Executive Board on data protection matters.
- Carries out a periodic review of the Data Protection Policy, with recommended changes being reported to Executive Board and Cabinet.
- Monitor compliance with the Council's Data Protection Policy.
- Create, maintain and publish the Councils Privacy Statement.
- Ensure regular training and guidance is available to employees and Councillors, and that it is up to date
- Advising the Council of its legal obligations in relation to the GDPR
- Informing, supporting and advising employees, Councillors and third parties (as appropriate) of their obligations and requirement of the GDPR.
- Monitoring compliance with the policy, reporting findings to Executive Board.
- Review of, maintaining logs of, and advising on privacy impact assessments.
- Provide standardised templates to managers on all GDPR notifications including notification of individuals' rights, consents, data sharing agreements, data audit forms and privacy impact assessment templates.
- To report any data breaches to the regulators and individuals
- Co-ordinating and responding to subject access requests and all other rights of individuals.
- Decision maker in relation to whether a subject access request is considered to be manifestly unfounded or excessive.
- Ensure sufficient organisational and technical policies are in place to protect personal data (and for the restoration of personal data where appropriate).
- Co-ordinate data protection audits and maintain records of the audits.
- Maintain a register of, and approve data sharing arrangements.
- Point of contact for, and working with the supervisory authority in relation to the processing of personal data.
- To maintain sufficient records (including all other registers and logs not identified separately above but set out in the policy) to demonstrate the Council is complying with the legislation.

Head of Public Health and Protection

- Maintenance of the Councils Patient Identifiable Information Policy and guidance.

Procurement Manager

- Provide advice and support with the DPO in contractual provisions with third parties.

Appendix B – Definitions

Data Subject

The data subject is the living individual to whom the person data relates.

Personal Data

Also known as Personal Information, or Personally Identifiable Information (PII), is information relating to a person, which can directly or indirectly identify that person. In particular, by reference to an identifier, such as a name, identification number, location data, online identifiers, or one or more factors specific to the identity of a person, such as physical, physiological, genetic, mental, economic, cultural or social identifiers.

Examples of this information can be names, addresses, passport number, IP addresses, photographs, nicknames, biometric data and health data.

Relevant Policies

There are a number of other policies and procedures integral to the governance framework for protecting data that employees must be aware of:

- The Data Protection Policy and associated policies, and Guidelines
- The Patient Identifiable Information Policy
- The Acceptable Use Policy for ICT
- The Use of Removable Media Policy
- The Disaster Recovery Policy
- The Information Protection Policy (IT)
- The Information Security Policy
- The IT Access Policy
- The IT Infrastructure Policy
- The Mobile Phone Security Policy
- The Remote Working Policy
- The Subject Access Requests Procedure
- The Data Breaches Procedure
- The Data Protection Training Procedure
- The Privacy Impact Assessment Procedure
- The Paper Records Handing Procedure
- The Secure Office Procedure

Sensitive Data

Also known as Sensitive Information or Sensitive Personal Data, are specific categories of personal data, which under the GDPR and other UK laws, explicit consent is required in order to hold and process. These categories of data are:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership (or lack of);
- Physical or mental health;
- Sex life and sexual orientation;
- Genetic data;
- Biometric data which can uniquely identify the individual;
- Actual or alleged criminal records, convictions or activities including court proceedings.

Third Parties

Any third party the Council legitimately shares, or that it intends to share data with, including, but not limited to contractors, service providers, partners and volunteers.

Data Controller – The term that describes those legal entities who collect and use Personal Data (in our scenario WHBC is the Data Controller)

A Data Controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. Where an organisation is required by law to process personal data, it must retain data controller responsibility for the processing. It cannot negate its responsibility by 'handing over' responsibility for the processing to another data controller or data processor.

NB. The term 'person' is a legal reference to a legal entity which is can include companies, public authorities or partnerships.

Data Processor – An external party who performs any activity whatsoever that involves Personal Data, held either electronically or manually, which is undertaken on behalf of the Data Controller. Sub-Data Processors can be appointed by the Data Processor but only with the permission of the Data Controller.

Protectively Marked Documents - The purpose of protective markings is to indicate the value of a particular asset in terms of the damage that is likely to result should it be compromised. The Protective Marking System ensures that sensitive information receives a uniform level of protection and treatment according to its degree of sensitivity.

Information Commissioner's Office - The Information Commissioner's Office is an independent authority in the UK that promotes openness of official information and protection of private information.

Appendix C – Councillors

This appendix sets out the various roles of Councillors in line with the Information Commissioners (ICO) guidance, and when this policy applies to Councillors.

More detailed guidance is available from the ICO:

https://ico.org.uk/media/for-organisations/documents/1432067/advice-for-elected-and-prospective-councillors.pdf

Councillors as a member of the Council

When Councillors receive and/or process information as a member of Council, they must comply with the Council's Data Protection Policies.

This includes all data and information shared by Officers as part of the Councils day to day operations, and any information received for and at Committee and Council meetings.

Councillors representing residents of their ward

Where a Councillors is acting in their capacity as a ward Councillor, they may process data in their own right, which the Council may not be aware, and may not be appropriate for it to be party to.

In these situations, a Councillor is acting as a data controller in their own right, and are required to be separately registered with the ICO. The Council has registered all Councillors as individual data controllers as requested by the ICO.

Councillors need to ensure they are aware of their responsibilities when sharing data with the Council and other parties, and feel comfortable that they have consent to share data from the constituent.

Should a Councillor receives information, which goes on to form part of the Councils day to day activities, this data should be managed in line with the Council's Data Protection Policies.

Councillors representing a political party

Councillors may process data on behalf of their political party, for example when using a mailing list for campaigning during elections.

When using data in this capacity, Councillors should comply with their parties' data protection policies and other relevant legislation (such as the Direct Marketing Legislation).