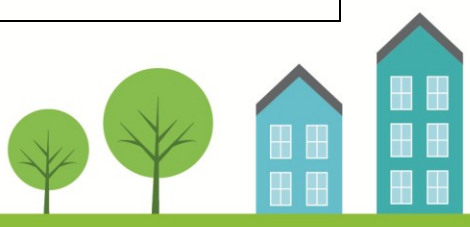
Data Protection Policy

Author	Cheryl Lincoln
Document Name	Data Protection Policy
Effective Date	May 2019
Review Date	October 2022
Version	V2.2



Havant BOROUGH COUNCIL

Data Protection Policy

Version Control

Version Number	Date	Author	Comments / Changes
v1.0	Feb 2010	Sarah Martin	Data Protection Policy under DPA98
v1.1	May 2018	Cheryl Lincoln	Minor Updates
V2.0	Jan 2019	Cheryl Lincoln	Re-write under GDPR and DPA18
v2.0	Mar 2019	Cheryl Lincoln	Approved by Information Governance Steering Group
V2.0	July 2019	Cheryl Lincoln	Approved by Corporate Governance Board
V2.1	Sept 2019	Cheryl Lincoln	Minor Update following Unison feedback
V2.2	Oct 2021	Cheryl Lincoln	Update to UK GDPR & Review Date

Dissemination

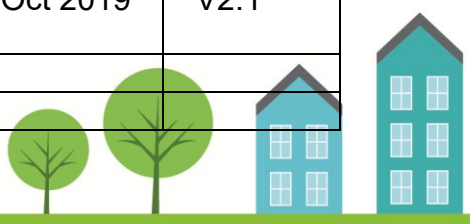
Who?	Method	Date	Version
Information Governance Steering Group	Steering Group Meeting	Mar 2019	V2.0
Corporate Governance Board	Corporate Governance Board Meeting	July 2019	V2.0
All Staff	Team Talk / Email to Team Managers	Jan 2020	V2.1

Publication of current version

Version	Location	Date
V2.1	Website (Policy Hub) / Intranet	Oct 19
V2.2	Website (Policy Hub) / Intranet	May 22

Approval of current version

Author / Reviewer	Who / Board	Date	Version
DPO	Corporate Governance Board & Joint HR Committee	Oct 2019	V2.1



Data Protection Policy

Contents

1	Policy Statement	3
2	About this Policy	3
3	Definition of Data Protection Terms	4
4	Responsibilities under the UK General Data Protection Regulation	5
5	Scope	6
6	Objectives	7
7	Data Protection Principles	7
8	Notifying Data Subjects	9
9	Data Security	9
10	Data Security Breaches	11
11	Disclosure and Sharing of Personal Information	11
12	Individual's Rights Under UK GDPR	11
13	Dealing with Subject Access Requests	12
14	Retention and Disposal of Personal Information	13
15	Use of CCTV	13
16	Freedom of Information / Environmental Information Regulations	13

1. Policy Statement

Everyone has rights regarding the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

Everyone who works for, and on behalf of, the Council for example Contractors, Agency Staff etc. are obliged to comply with this policy when processing personal data on our behalf.

2. About This Policy

The types of personal data that the Council may be required to handle include information about current, past and prospective customers and others that we communicate with. Personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 (together referred to as the Data Protection Legislation).

This policy, along with the Council's Privacy Notice and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources and in accordance with the Data Protection Legislation.

This policy has been approved by the Council's Corporate Governance Board. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

The Data Protection Officer is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer at dp@havant.gov.uk

The Data Protection Officer is registered with the Information Commissioners Officer (ICO) and is responsible for registering the council with the ICO. The ICO is the independent regulatory office in charge of upholding information rights in the interest of the public.

3. Definition of Data Protection Terms

3.1 Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.2 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, a unique reference number, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.3 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is

processed. They are responsible for establishing practices and policies in line with UK GDPR. The Council is the data controller of all personal data it collects or uses in its day to day business and in providing services.

3.4 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition, but it includes suppliers, providers and contractors which handle personal data on the council's behalf.

3.5 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, viewing, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.6 **Special Category Data** (also known as "sensitive personal data") includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. The definition also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation. Special Category Data can only be processed under strict conditions. Personal Data relating to criminal convictions and offences is subject to additional requirements and should be handled in a similar way to Special Category Data.

3.7 **Third Party** - Any individual/organisation other than the data subject, the data controller (the council's) or its agents.

4. Responsibilities under The UK General Data Protection Regulations (UK GDPR)

4.1 The Council is a Data Controller under UK GDPR; it is also a Processor of information for other organisations.

4.2 The Information Governance Manager is the appointed Data Protection Officer (DPO) as defined under the UK General Data Protection Regulation (UK GDPR). The regulation specifies the minimum duties or "tasks" to be performed by the DPO.

- To inform and advise the Council, and their employees, of their obligations under the Regulation and other applicable laws and regulations.
- To monitor compliance with the Regulation and other applicable laws and regulations and with the relevant policies of the Council data controller, this includes assignment of responsibilities, awareness and training, and relevant audits.

- To advise on the Data Protection Impact Assessment (DPIA) process and monitor its performance, if requested.
- To liaise with the Information Commissioner's Office as required (Article 39(1)(a)-(e).

4.3 The Information Governance Team, through the Information Governance Steering Group, is responsible for developing and encouraging good information handling practice within the Council. The Information Governance Steering Group provides a quarterly report to the Corporate Governance Board

4.4 Compliance with data protection legislation is the responsibility of everybody who processes personal information however;

Managers/Team Leaders within every business area are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties.

Managers must always contact the Data Protection Officer if:

- they are unsure of the lawful basis which they are relying on to process personal data;
- they need to rely on consent for processing personal data;
- they need to prepare privacy notices or other transparency information;
- they are unsure about the retention period;
- they are unsure on what basis to transfer personal data outside the United Kingdom;
- they are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment;
- they plan to use personal data for purposes other than those for which it was originally collected;
- they plan to carry out activities involving automated processing including profiling or automated decision-making;
- they need help with any contracts or other areas in relation to sharing personal data with third parties (including our contractors);
- they plan to share data with another organisation or person in a way which is new or could affect data subjects' rights;

4.5 The Council through its staff is responsible for ensuring that any personal data supplied is accurate and up-to-date.

5. Scope

This policy must be followed by all staff who work for or on behalf of the Council including those on temporary contracts, secondments, volunteers, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services.

This policy is applicable to all areas of the organisation and covers all aspects of information including (but not limited to):

- Service user information.
- Personnel/Staff information.
- Organisational and business sensitive information.
- Structured and unstructured record systems - paper and electronic.
- Photographic images, digital, text or video recordings including CCTV, BWC.
- All information systems purchased, developed and managed by/or on behalf of, the organisation.
- Information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras.

The processing of all types of information, including (but not limited to):

- Organisation, adoption or alteration of information.
- Retrieval, consultation, storage/retention or use of information.
- Disclosure, dissemination or otherwise making available information for operational or legal reasons.
- Alignment, combination/linkage, blocking, erasing or destruction of information.

Failure to adhere to this policy may result in disciplinary action, for example where it is deemed to be serious e.g. deliberate or malicious actions and where necessary referral is required to the appropriate regulatory bodies e.g. ICO or the police

6. Objectives

The Council will, through appropriate management, and strict application of criteria and controls to:

- observe fully conditions regarding the fair and lawful collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information to the extent that it is needed to fulfil operational needs or to comply with legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Legislation;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred outside the UK without suitable safeguards.

7. Data Protection Principles

Anyone processing personal data must comply with the six principles relating to processing of personal data in the UK GDPR. These provide that personal data must be:

7.1 **Processed lawfully, fairly and in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency').

For personal data to be processed lawfully, it must be processed on the basis of one of the legal grounds set out in UK GDPR. These include, among other things, 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;
- for the performance of a contract to which the data subject is party;
- for compliance with a legal obligation or duty;
- the data subject has given consent for the data to be processed for a specific purpose(s).

When special category data (sensitive personal data) is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

7.2 **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes.

We will only process personal data for the specific purposes set out in the Council's Record of Processing Activities (RoPA) or for any other purposes specifically permitted by the legislation. We will notify those purposes to the data subject when we first collect the personal data or as soon as possible thereafter.

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

Personal data, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If personal data is given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

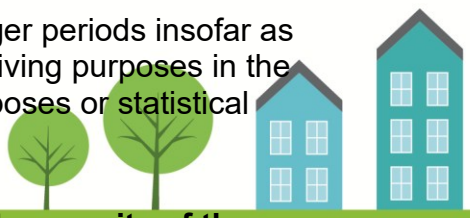
7.4 **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

Personal Data, which is kept for a long time, must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that personal data held by the council is accurate and up-to-date. Individuals should notify the council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Council to ensure that any notification regarding change of circumstances is noted and acted upon.

7.5 **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.

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

On occasion, 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).



7.6 **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').

8. Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them through our Privacy Notices about:

a. The purpose or purposes for which we intend to process that personal data.
b. The legal basis for processing.
c. The types of third parties, if any, with which we will share or to which we will disclose that personal data.
d. Refer them to the Retention Schedule which sets out the length of time that we will retain the data.
e. The means, if any, with which data subjects can limit our use and disclosure of their personal data.
f. If we receive personal data about a data subject from other sources, we will provide the data subject with this information within the required timescales.
g. We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and the contact details of our Data Protection Officer.

9. Data Security

9.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

9.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

9.3 Personal data will only be transferred to a data processor who has provided sufficient guarantees to implement appropriate technical and organisational measures that will comply with the Data Protection legislation and ensure that data subjects rights are protected and that these requirements are governed by a contract or other legally binding agreement.

9.4 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) Confidentiality means that only people who are authorised to use the personal data should access it.

b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

c) Availability means that authorised users should be able to access the personal data if they need it for authorised purposes.

9.5 Security procedures include:

a) Entry controls. Any stranger seen in entry-controlled areas will be reported.

b) Secure lockable cupboards. Desks and cupboards will be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

c) Methods of disposal. Paper documents will be shredded. Digital storage devices will be physically destroyed when they are no longer required.

d) Equipment. Council employees will ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

e) IT Security. The Council will ensure their IT providers maintain up to date firewalls, patching and other IT security measures.

9.6 Training for staff includes:

(a) Mandatory training for all staff on Data Protection and Cyber Security with annual refresher training.

(b) Training for specialist Data Protection staff, including those who handle Subject Access Requests.

(c) Training before access is provided to data systems.

9.7 Governance and Assurance Procedures include:

(a) An Information Governance framework overseen by the Data Protection Officer.

(b) The appointment of a Senior Information Risk Officer (SIRO), with cross organisational oversight provided by the Council's Corporate Governance Board.

(c) The regular audit of the council's Information Management processes and procedures.

10. Data Security Breaches

Any data security breaches must follow the Councils Data Incident Report Plan. Ultimately the Data Protection Officer will consider whether the risk poses a risk to people, taking account of the likelihood and severity of any risk to people's rights and freedoms, following the breach. If the Data Protection Officer makes this assessment, if they feel it's likely there will be a risk then they will inform the SIRO (and in the absence of the SIRO the Chief Executive) and notify the ICO, taking account of the 72 hours the Council has to report personal data breaches.

11. Disclosure and Sharing of Personal Information

We will only disclose or share a data subject's personal data where we are legally permitted to do so, in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

On occasions where we decide to share a data subject's personal data, we will ensure that only the minimum amount of relevant information is shared; and that the provisions of DPA 2018, UK GDPR and other privacy laws have been satisfied.

12. Individual's Rights Under Data Protection legislation

Individuals have a number of rights including the right to: -

- ask the Council if it holds personal information about them

- ask what it is used for
- be given a copy of the information (subject to certain exemptions)
- be given details about the purposes for which the Council uses the information and of other organisations or persons to whom it is disclosed.
- ask for incorrect data to be corrected.
- be given a copy of the information with any unintelligible terms explained;
- be given an explanation as to how any automated decisions taken about them have been made.
- ask that information about them is erased ("right to be forgotten")
- ask the Council not to use personal information: -
    - for direct marketing; which is likely to cause unwarranted substantial damage or distress;
    - to make decisions which significantly affect the individual, based solely on the automatic processing of the data.

These rights are not absolute, if the Council is unable to respond to a request, it will outline the legal reasons for its decision clearly.

Further details, including how to exercise your rights, can be found in Data Subject Rights guidance.

13. Dealing with Subject Access Requests

The Council has provided application forms on its website to assist data subjects to make a request to access information we hold about them. There are some limited circumstances in which personal data relating to the applicant may be withheld. Examples of this include repeat access requests, confidential references, and third-party information.

Requests can be made both verbally and in writing, they do not need to state that it is a Subject Access Request, however anyone who is asking for a copy of their own data/information should be referred to the Information Governance team.

Any individual who wishes to exercise this right should provide satisfactory proof of identity and, enough information to enable the data to be located. Subject to satisfactory completion of the above, the council should respond within one month of receipt of above and in accordance with any relevant exemptions specified in the legislation.

14. Retention and Disposal of Data

The council discourages the retention of personal data for longer than they are required. Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

The council maintains Retention Schedules that are specific and relevant to specific types of information and the services they relate to. These outline the appropriate periods for retention.

15. Use of CCTV

The council's use of CCTV is regulated by the Surveillance Camera Commissioner. The council complies with the Surveillance Camera Code of Practice and the ICO Code of Practice, supplemented by local policy and guidance.

16. Freedom of Information Act 2000 / Environmental Information Regulations (EIR) 2004

The Freedom of Information Act 2000 (FOIA) allows public access to all types of information held by public authorities, with the exception of personal information. Requests for personal information will be dealt with under the Data Protection Act. For more information on both the FOIA and EIR please refer to our Access to Information Policy.