HARTLEPOOL BOROUGH COUNCIL

DATA PROTECTION POLICY

(July 2018)

Document Control

Organisation	Hartlepool Borough Council
Title	Data Protection Policy
Author	Laura Stones
Date created	July 2018
Next review date	July 2019

Revision History

Revision Date	Reviser	Version	Description of Revision

Document Approvals

Version	Approved by	Date approved
1.1	Finance and Policy Committee	30 July 2018

1. Introduction

1.1 This Data Protection Policy sets out how Hartlepool Borough Council handle the Personal Data of its customers, suppliers, employees, and other third parties, in line with the provisions set out in the General Data Protection Regulation (GDPR).

1.2 This Policy applies to all personal data the Council processes regardless of where the data is stored or whether it relates to past or present employees, customers, clients or supplier contacts, website users or any other Data Subject.

1.3 The Council robustly complies with the GDPR from 25 May 2018.

2. Policy Aims

2.1 The aims of this policy are:

(a) To ensure that the Council captures, stores, processes and disposes of personal information in a lawful, ethical and responsible way.

(b) Respect the rights of individuals where personal data is processed.

3. Scope

3.1 The correct and lawful treatment of personal data will maintain confidence in the organisation. Protecting the confidentiality and integrity of personal data is a critical responsibility that the Council take seriously at all times. The Council is exposed to potential fines of up to 20 million Euros (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

3.2 Hartlepool Borough Council is responsible for:

(a) The overall responsibility for the efficient administration of data protection legislation

3.3 The Council's Corporate Management Team is responsible for:

a) Promoting and supporting arrangements to deliver effective data protection compliance.

b) Monitoring the on-going effectiveness of the management processes.

c) Ensuring there is an appointed Data Protection Officer.

3.4 The Data Protection Officer is responsible for:

a) Day to day administration and compliance with data protection legislation.

b) Establishing appropriate governance structures to implement and monitor data protection arrangements across the Council.

c) Ensuring that this policy is followed in a consistent manner.

d) Communicating this policy to employees.

3.5 All Managers are responsible for:

a) Actively promoting the Data Protection Policy and its principles and take steps to implement improvements to work processes within their own area of functional responsibility.

b) Ensuring that staff under their direction and control are aware of the policies, procedures and guidance laid down and for checking that those staff understand and appropriately apply policies, procedures and guidance in respect of information governance in carrying out their day to day work.

c) Taking steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on ICT equipment is protected by the use of secure passwords, which have forced changes periodically.
- Individual passwords should be such that they are not easily compromised.

d) Managers are also responsible for ensuring all staff within their functional areas have had training appropriate to their roles and

that this is current.

3.6 All employees are responsible for:

a) Acquainting themselves with and abiding by the data protection principles.

b) Reading the Data Protection Policy and understanding how it impacts on their role.

c) Understanding how to conform to the policy in relation to the retention of personal data.

d) Understanding how to conform to the policy in relation to safeguarding Data Subjects' rights.

e) Understanding what is meant by special categories of personal data and how to handle such data.

f) Contacting the Data Protection Officer if there is any doubt so as not to jeopardise individuals' rights or risk contravention of the regulations.

g) Ensuring they have had data protection training on induction to the organisation and completed a refresher annually.

3.7 All contractors, consultants, partners or agents of the Council must:

a) Ensure that they and all their staff who have access to personal data held or processed for or on behalf of the Council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Council and that individual, company, partner of firm.

b) Allow data protection audits by the Council of data held on its behalf (if requested).

c) Ensure all contractors who are users of personal information supplied by the Council confirm that they will abide by the requirements of the Act with regard to the information supplied by the Council.

4. Data Protection Principles

4.1 The GDPR provides conditions for the processing of any personal data. They also make a distinction between personal data and special categories of personal data.

4.2 Personal data is defined as, data relating to a living individual who can be identified from:

a) that data.

b) that data and other information which is in the possession of, or is likely to come into the possession of the Data Controller and includes an expression of opinion about the individual and any indication of the intentions of the Council, or any person in respect of the individual.

4.3 Special categories of personal data consist of:

a) Racial or ethnic origin.

b) Political opinion.

c) Religious or other beliefs.

d) Trade union membership.

e) Physical or mental health or condition.

f) Sexual life.

g) Genetic or biometric data.

h) Criminal convictions and offences.

4.4 In the GDPR regulations:

a) Data Subject means an individual who is the subject of personal data

b) Data Controller means a person who either alone or jointly or in common with other persons determines the purpose for which and the manner in which any personal data are, or are to be processed.

c) Data Processor, in relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

4.5 The Council adhere to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

d) Accurate and where necessary kept up to date (Accuracy).

e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.6 The Council are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Lawfulness, fairness, transparency

5.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2 The Council may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the Data Subject.

5.3 The GDPR allows Processing for specific purposes, as set out below:

a) The Data Subject has given his or her consent.

b) The Processing is necessary for the performance of a contract with the Data Subject.

c) To meet our legal obligations.

d) To protect the Data Subject's vital interests.

e) 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 controller.

f) To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices (Local Authorities cannot rely on this processing ground).

5.4 You must identify and document the legal ground being relied on for each processing activity.

Consent

5.5 A Data Controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR.

5.6 A Data Subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

5.7 Data Subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

5.8 Unless the Data Controller can rely on another legal basis of processing, explicit consent is usually required for processing special categories of personal data, for automated decision-making and for cross border data transfers. Usually, another legal basis can be relied upon (and not require explicit consent) to process most types of special categories of data. Where explicit consent is required, a privacy notice to the Data Subject to capture explicit consent must be issued.

5.9 All consents must be recorded so that the Council can demonstrate compliance with consent requirements.

Transparency (notifying Data Subjects)

5.10 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

5.11 Whenever the Council collects personal data directly from Data Subjects, including for human resources or employment purposes, the Council must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why the Council will use, process, disclose, protect and retain that personal data through a Privacy Notice which must be presented when the Data Subject first provides the personal data.

5.12 When personal data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates the proposed processing of that personal data.

6. Purpose limitation

6.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

6.2 Personal data for new, different or incompatible purposes from that disclosed when it was first obtained cannot be processed, unless the Data Subject is informed of the new purposes and they have consented, where necessary.

7. Data minimisation

7.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When personal data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the Council's Retention Policy.

8. Accuracy

8.1 Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. Personal data must be checked for accuracy at the point of collection and at regular intervals afterwards. All reasonable steps to amend inaccurate or out-of-date personal data must be made.

9. Storage limitation

9.1 Personal data must not be kept in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirements.

9.2 It is a requirement to inform Data Subjects in privacy notices regarding the retention periods for data.

10. Security, integrity and confidentiality

Protecting Personal Data

10.1 Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

10.2 The Council has developed, implemented and maintained safeguards including use of encryption and Pseudonymisation where applicable. The Council will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

10.3 The confidentiality, integrity and availability of personal data must be protected (definitions below):

a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

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

c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

11. Reporting a Personal Data Breach

11.1 The GDPR requires Data Controllers to notify any personal data breach to the Information Commissioner's Office within 72 hours and, in certain instances, the Data Subject.

11.2 A personal data breach is a "*breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data* "

11.3 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact your Information Governance Representative. You should preserve all evidence relating to the potential personal data breach.

12. Transfer limitation

12.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. If a transfer of data is required to countries outside the EEA, contact your Information Governance Representative before the transfer is made.

13. Data Subject's rights and requests

13.1 Data Subjects have rights when it comes to how we handle their personal data.

These include rights to:

a) Withdraw consent to processing at any time.

b) Receive certain information about the Data Controller's processing activities.

c) Request access to their personal data that we hold.

d) Prevent our use of their personal data for direct marketing purposes.

e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data.

f) Restrict processing in specific circumstances.

g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest.

h) Request a copy of an agreement under which personal data is transferred outside of the EEA.

i) Object to decisions based solely on Automated Processing, including profiling.

j) Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else.

k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.

l) Make a complaint to the supervisory authority.

m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

13.2 Notify your Information Governance Representative of any Data Subject requests and send a copy of the request to **dataprotection@hartlepool.gov.uk**

14. Accountability

14.1 The Council must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Council is responsible for, and must be able to demonstrate, compliance with the data protection principles.

14.2 The Council has adequate resources and controls in place to ensure and to document GDPR compliance including:

a) Appointing a suitably qualified DPO.

b) Implementing privacy by design when processing personal data and completing Data Protection Impact Asessments (DPIA) where processing presents a high risk to rights and freedoms of Data Subjects.

c) Integrating data protection into internal documents, related policies, privacy guidelines, privacy notices.

d) Regularly training staff on the GDPR, related policies and privacy guidelines and data protection matters including, for example, Data Subject's rights, consent, legal basis, DPIA and personal data breaches. The Council must maintain a record of training attendance by staff.

e) Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

15. Record keeping

15.1 The GDPR requires the Council to keep full and accurate records of all data processing activities.

15.2 The Council must keep and maintain accurate corporate records reflecting the processing activities including records of Data Subjects' consents and procedures for obtaining consents.

15.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the personal data types, Data Subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

16. Training and Audit

16.1 The Council are required to ensure all staff have undertaken adequate training to enable them to comply with the GDPR. The Council must also regularly test systems and processes to assess compliance.

16.2 The Council must regularly review all the systems and processes to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

17. Privacy By Design and Data Protection Impact Assessment (DPIA)

17.1 The Council are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data protection principles.

17.2 The Council must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

a) The state of the art;

b) The cost of implementation;

c) The nature, scope, context and purposes of processing; and

d) The risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

17.3 The Council must also conduct DPIAs in respect to high risk processing. A template is available from the DPO.

17.4 A DPIA must be conducted (and findings discussed with the DPO) when implementing major system or business change programs involving the processing of personal data including:

a) Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes).

b) Automated processing including profiling and ADM.

c) Large-scale processing of sensitive data; and

d) Large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

a) A description of the processing, its purposes and the Data Controller's legitimate interests if appropriate.

b) An assessment of the necessity and proportionality of the processing in relation to its purpose.

c) An assessment of the risk to individuals.

d) The risk mitigation measures in place and demonstration of compliance.

18. Automated Processing (including profiling) and Automated Decision-Making (ADM)

18.1 Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

a) A Data Subject has explicitly consented;

b) The processing is authorised by law; or

c) The processing is necessary for the performance of or entering into a contract.

18.2 If certain types of sensitive data are being processed, then grounds (b) or (c) will not be allowed but such sensitive data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

18.3 If a decision is to be based solely on automated processing (including profiling), and then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

18.4 The Council must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

18.5 A DPIA must be carried out before any automated processing (including profiling) or ADM activities are undertaken.

19. Direct marketing

19.1 The Council are subject to certain rules and privacy laws when marketing to customers. For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls).

19.2 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

19.1 A Data Subject's objection to direct marketing must be promptly honoured.

20. Sharing Personal Data

20.1 Generally, the Council are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

20.2 The Council may only share the personal data we hold with third parties, such as our service providers if:

a) They have a need to know the information for the purposes of providing the contracted services.

b) Sharing the personal data complies with the privacy notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained.

c) The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

d) The transfer complies with any applicable cross border transfer restrictions.

e) A fully executed written contract that contains GDPR approved third party clauses has been obtained.

21. Further details

21.1 Contact your Information Governance Representative if you are:-

a) Unsure of the lawful basis which you are relying on to process Personal Data).

b) Need to rely on consent and/or need to capture explicit consent.

c) If you need to draft privacy notices.

d) If you are unsure about the retention period for the personal data being processed.

e) If you are unsure about what security or other measures you need to implement to protect personal data.

f) If there has been a data breach or a suspected data breach.

g) If you need to transfer data outside the EEA.

h) If you need any assistance dealing with any rights invoked by a Data Subject.

i) Whenever you are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment or plan to use personal data for purposes other than what it was collected for.

j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making.

k) If you need help complying with applicable law when carrying out direct marketing activities.

l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

22.2 Contact details for the Information Governance Group are as follows:

Adult and Community-Based Services	Trevor Smith 523950
Children's and Joint Commissioning	Kay Forgie 284119
Public Health	Michelle Chester 852837
Regeneration & Neighbourhoods Department	Steve Russell 523031

Chief Executive's Department / Corporate ICT	Paul Diaz 284280
Internal Audit	Sharon Bramley 07825 272790
Chief Executive's (Finance)	Carol Purdy 525200
Human Resources	Christopher Pendlington 284039
Legal/Data Protection Officer	Laura Stones 523087