MEETING OF FULL TOWN COUNCIL MONDAY 10 JULY 2023

APPENDICES FOR PAPER C - REVIEW OF GDPR DOCUMENTS

Policies and Procedures

This page is intentionally left blank.

Appendix 1

DATA PROTECTION POLICY

Hertford Town Council

Version March 2023

INTRODUCTION

Hertford Town Council ("the Council") needs to process personal information (electronic or paper based) about individuals in order to provide various public services to our community. It is also necessary to process personal information about our staff and others who we come into contact with during the course of our operations. In doing so, we recognise that the correct and lawful treatment of personal information is critical to maintaining the trust and confidence of those connected to us.

This policy, and any other documents referred to in it, sets out our approach to ensuring that we comply with data protection laws. It has been prepared and updated to take account of changes in the law introduced by the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR") and the Data Protection Act 2018 ("DPA"). In particular, a key change introduced is the principle of 'accountability' which requires us to demonstrate how we comply with data protection laws.

All staff (including employees, officers, workers, and consultants) must comply with our policies and procedures relating to data protection. This policy does not form part of any employee's contract of employment and may be amended at any time.

DATA PROTECTION PRINCIPLES

We are committed to processing personal data in accordance with the 6 key data protection principles outlined in the GDPR:

1. LAWFULNESS, FAIRNESS AND TRANSPARENCY

a. **Transparency:** We will tell data subjects how we will use their personal information.

b. **Fairness:** We will ensure that we process personal information fairly; only using that information for the purposes set out in our privacy information or in a way which is compatible with those purposes.

c. **Lawfulness:** we will ensure that we have identified a lawful basis for processing personal information.

2. PURPOSE LIMITATION

Personal data will only be obtained for "specified, explicit and legitimate purposes". Personal Data will only be used for a specific processing purpose that the data subject has been made aware of.

3. DATA MINIMISATION

Personal data collected about a data subject will be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

4. ACCURACY

We will develop processes and protocols that support data being "accurate and where necessary kept up to date".

5. STORAGE LIMITATIONS

Personal data will be "kept in a form which permits identification of data subjects for no longer than necessary".

6. INTEGRITY AND CONFIDENTIALITY

We are committed to handling data "in a manner ensuring appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage".

DATA INFORMATION OFFICER

We have appointed a 'Data Information Officer' ("DIO"). The DIO must have expert knowledge in data protection law and practices. Our appointed DIO is HY Solicitors, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL who can be contacted by telephone on 0161 804 1144 or email at DPO@wearehy.com

RESPONSIBILITIES

Everybody has a responsibility to ensure compliance with the GDPR and DPA. As part of our commitment to ensuring that we comply with our data protection obligations, particularly the principal of accountability, the Council has established where responsibilities are assigned:

The Town Clerk

- ensure that a suitably qualified DIO is appointed
- include budget and resources needed to ensure compliance at all levels
- comply with all reasonable directions from the DIO to promote effective data protection practices
- ensure that staff receive appropriate training at reasonable internals in relation to data protection
- ensure that the appropriate policies and procedures are implemented which demonstrate how the Council complies with its data protection obligations
- ensure that Privacy Notices are readily available
- ensure that an Article 30 register is held and kept up to date
- ensure that data protection impact assessments are undertaken when required

The DIO

- support the Town Clerk to comply with their responsibilities
- update and maintain data protection policies and procedures
- provide advice in respect of data protection impact assessments
- update privacy notices
- investigate and report on data breaches
- liaise with the ICO in relation to all compliance matters
- provide advice and support across the Council on all matters which impact on individual rights
- provide training where requested to do so

Staff

- Observe data protection policies, procedures and guidance implemented by the Council
- understand the purposes for which the Council uses personal information
- collect and process appropriate information in accordance with the purposes for which it is to be used
- ensure that information is correctly input into systems
- ensure that information is destroyed (in accordance with our retention procedures) when it is no longer required
- on receipt of a request from an individual or organisation for information held about them or another data subject, immediately notify the DIO in accordance with the subject access procedure
- attend training when required to do so
- understand that breaches of this policy may result in disciplinary action, including dismissal

IMPLEMENTATION

This policy will be implemented and supported through the development of a data protection framework comprising of 2 elements:

Data Protection - Standards

- The Standards set out the actions that will be taken to implement the data protection policy

Procedures

- Step by step instructions to achieve a given aspect of the standards

Data Protection – Standards

Purpose

The Standards outline the actions that will be taken to implement the data protection policy and cover the following areas of data protection:-

S1: Lawfulness, fairness and transparency
S2: Individual Rights
S3: Accountability and governance
S4: Information security
S5: Physical Security
S6: Computer and network security
S7: Personal data breach management
S8: Records management
S9: Access to records
S10 Communication using email
S11: Training and Awareness

S1: Lawfulness, fairness and transparency

- We will conduct information audits at appropriate intervals and maintain a record of processing activities in compliance with Article 30 of the GDPR ("the Record")
- The Record will document the personal data processes undertaken, its purpose, where it comes from and who we share data with
- We will identify the lawful bases for processing and document it in the Record
- We will keep a record of consent
- Where we rely on legitimate interests as the lawful basis for processing, we will apply the three-part test and demonstrate that we have considered and protected individual's rights and interests
- We will register with the Information Commissioners Office

S2: Individual Rights

- We will provide privacy information to individuals
- We will communicate privacy information in a way that is clearly understood and accessible
- We will have a process to recognise and respond to individual requests to access their personal data

- We will have processes in place to ensure that the personal data we process remains accurate and up to date
- We will have processes in place to securely dispose of personal data that is no longer required or where an individual has asked us to erase it.
- We will have procedures to respond to an individual's request to restrict the processing of their personal data
- We will have procedures to allow individuals (where applicable) to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability
- We will have procedures to handle an individual's objection to the processing of their personal data

S3: Accountability and governance

- We will have a data protection policy
- The data protection policy will be supported by a framework which details how we will respond to subject access requests, handle data breaches, provide privacy information and how long we will retain personal data
- We will provide data protection awareness training for all staff
- We will have written contracts with any processors that we use
- An Article 30 register will be maintained
- We will use the principles of 'Data protection by Design and Default' and implement appropriate technical and organisational measures to integrate data protection into our processing activities
- We will conduct Data Protection Impact Assessments (DPIAs)
- We will have a nominated Data Information Officer (DIO)
- Decision makers and key people will demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the Council

S4: Information security

- We will identify, assess and manage information security risks
- We will have established written agreements with third-party processors that ensure the personal data that they access and process on our behalf is protected and secure

- We will ensure that we have an adequate level of protection for any personal data processed by others on our behalf that is transferred outside the European Economic Area

S5: Physical Security

- We will have entry controls to restrict access to premises and equipment in order to prevent unauthorised physical access, damage and interference to personal data
- We will have secure storage arrangements to protect records and equipment in order to prevent loss, damage or theft of personal data
- We will have a process to securely dispose of records and equipment when no longer required and this will be done safely such that the data is irrecoverable

S6: Computer and network security

- We will assign user accounts to authorised individuals and will manage user accounts effectively to provide the minimum access to information
- We will have appropriate password security in place
- We will establish effective anti-malware defences to protect computers from malware infection
- We will routinely back-up electronic information to help restore information in the event of disaster
- We will keep software up-to-date and apply the latest security in order to prevent the exploitation of technical vulnerabilities
- We will have boundary firewalls to protect computers from external attack and exploitation and help prevent data breaches

S7: Personal data breach management

- We will have an effective process to identify, report, record, manage and resolve any personal data breaches
- We will have training in place to ensure staff know how to recognise and what to do if they detect a personal data breach
- We will have a procedure in place to report a breach to the ICO and to affected individuals, where necessary
- We will have a procedure in place to effectively investigate the cause(s) of a breach and implement measures to mitigate future risks

S8: Records management

- We will have a records management policy
- We will implement processes to ensure that personal data is held in accordance with the records management policy

S9: Access to records

- We will implement role-based access and check it regularly
- We will have a process to assign and manage user accounts to authorised individuals and to remove them when no longer appropriate

S10: Use of email

- Each e-mail user will be allocated their own personal account with a unique identifier and password
- Industry recognised e-mail software will be installed and kept up to date
- All emails that are used for official business will be sent from an official domain address
- A standard disclaimer to protect the Council against any liability and the unauthorised disclosure of the contents of e-mails will be automatically appended to each e-mail
- Sensitive personal information will only be sent via email if there is a method in place to ensure the information is secure. This includes either:
    - Sending the information as a password protected attachment or
    - Providing a link to a secure shared area document
- The use of e-mail will be monitored to protect against misuse

S11: Training and Awareness

- To ensure all staff are aware of their responsibilities under the GDPR and are aware of associated policies and procedures, appropriate training will be provided for all those involved in using our data and systems
- All staff will receive notification regarding changes to policies, standards and procedures on a timely basis

Appendix 1

Data Protection – Procedures

We will maintain the following procedures to support the Data Protection Standards

P1: Subject Access Requests (SARs)

P2: Data Breach Procedure

P3: Records Management Policy

Document 6.7

INFORMATION AND DATA PROTECTION POLICY

(Includes the Policy, Responsibilities and Guidance)

Adopted May 2018
Review by June 2023

1 Introduction

1.1 This Policy sets out how the Council handles Personal Data it processes in order to deliver many of the services and functions carried out, whether that be about 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 in order to comply with the requirements of central government. We have updated our policy to take account of changes in the law brought about by the General Data Protection Regulation ("The GDPR") and the Data Protection Act 2018.

1.2 This Policy applies to all Personnel ("you", "your"). Data protection is a collective responsibility and all Personnel are required to demonstrate good data protection practices to support us in creating a strong culture of data protection compliance. Any breach may result in disciplinary action and, where data Processors and sub-processors are concerned, termination of our relationship.

2 Statement of Policy

2.1 This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means such as audio and visual, and there are safeguards within the Act to ensure this.

2.2 The Council regards the lawful and correct 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.

2.3 The Council will ensure that it treats personal information lawfully and correctly.

2.4 The Data Protection Act defines what is a public authority for the purposes of GDPR. The Council is not a public authority within the definitions of the Data Protection Act however, the Council is still subject to data protection legislation.

2.5 The Council has appointed a Data Information Officer to assist the Council in overseeing this policy. The DIO is HY Professional Services ("HY") who can be contacted as follows:-

In writing: HY, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL
By email: DPO@wearehy.com
By telephone: 0161 804 1144.

2.6 Please contact the DIO with any questions about the operation of this Policy.

3 The Principles of Data Protection

3.1 The GDPR stipulates that the Council in processing personal data must comply with **six principles**.

3.2 The Principles require that personal information shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- kept in a form which permits identification of data subjects for no longer than is necessary;
- processed so as to ensure appropriate security of the personal data, including against unauthorised or unlawful processing and against accidental loss, destruction or damage. There is some special provision, including for public interest archiving and historical research.

3.3 The GDPR provides conditions for the processing of any personal data. Personal data is defined as any information relating to an identified or identifiable living individual

4 Management of Personal Data

4.1 The Council will, through appropriate management and the use of guidance from the Information Commissioner:-

- fully meet requirements regarding the collection and use of personal information;
- meet its legal obligations to specify the purpose for which information is used;
- collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards;
- ensure that the rights of people about whom the information is held can be fully exercised under the Act and the GDPR.

These include:

- the right to be informed that processing is being undertaken;
- the right of access to one's personal information within the statutory 30 days;
- the right to prevent processing in certain circumstances;
- the right to correct, rectify, block or erase information regarded as wrong information;
- the right to object - processing has to be based on legitimate interests or the performance of a task in the public interest/exercise of official authority;
- rights related to direct marketing (including profiling.

4.2 In addition, the Council will ensure that:

- the Town Clerk has overall responsibility for data protection in the Council;
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- everyone managing and handling personal information is appropriately trained to do so;

- everyone managing and handling personal information is appropriately supervised;
- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are periodically assessed and evaluated;
- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will comply with approved procedures;
- all elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act and the GDPR;
- all staff will take 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 computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
    - individual passwords should be such that they are not easily compromised;
    - passwords should not be written down;

- all contractors, consultants, partners or other servants or agents of the Council must:

    - ensure that they and all of 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 GDPR. 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 or firm;
    - allow data protection audits by the Council of data held on its behalf (if requested);
    - indemnify the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation;

- all contractors who are users of personal information supplied by the Council will be required to confirm that they will abide by the requirements of the Act and the GDPR with regard to information supplied by the Council

5 Implementation

5.1 The Council has identified the Town Clerk as the officer responsible for ensuring that the Data Protection Policy is implemented. In the first year of implementation the process will be monitored quarterly by the Council via a report to the Finance, Policy & Administration Committee. After the first year the report will be submitted annually.

5.2 The Town Clerk will also have overall responsibility for:

- the provision of data protection training for Councillors and Council Staff

- ensuring compliance checks are carried out to ensure adherence with the GDPR.

6. Notification to the Information Commissioner

6.1 The Information Commissioner maintains a public register of data controllers.

6.2 The Council is registered as a data controller[1].

[1] The Data Controller is a person who (either alone or jointly or in common with other persons – i.e. the Council) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

This page is intentionally left blank.

SUBJECT ACCESS PROCEDURE

Hertford Town Council

Version March 2023

INTRODUCTION

Hertford Town Council ("the Council") needs to process personal information (electronic or paper based) about individuals in order to provide services in our community. It is also necessary to process personal information about our staff and others who we come into contact with during the course of our operations. In doing so, we recognise that the correct and lawful treatment of personal information is critical to maintaining the trust and confidence of those connected to us.

This policy sets out our approach to ensuring that data subjects are able to request and access personal data which we hold about them in accordance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA).

DEFINITION

A Subject Access Request (SAR) is any request made by an individual for personal information that we hold about them. A SAR gives a data subject the right to receive a copy of their own personal data unless there is an exemption which allows us to withhold access.

PROCESS

Our response to a subject access request will involve the following four elements:-

1. Initial response
2. Identity verification
3. Gathering information
4. Review
5. Response

Guidelines for each step are outlined in appendices 1 to 5

Appendix 1: Initial Response Guidelines

Upon receipt of a SAR, the Council will send an acknowledgment letter to the requester. A template letter and initial advice may be obtained from the Data Information Officer ("DIO"), HY Solicitors, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL by email to DIO@wearehy.com or by telephoning 0161 8041144.

Appendix 2: Identity Verification Guidelines

Before disclosing any personal information, the person receiving the request must verify the identity of the data subject. The DIO will provide advice as to whether identification is necessary. The Council may, if appropriate, ask the requester to provide one form of photograph ID such as a passport or driving licence and one of form of proof of address such as a utility bill.

Appendix 3: Gathering Information Guidelines

The DIO, if requested to do so, will direct the Council as to the enquiries that it needs to conduct as part of a reasonable search for the requested personal information. In complex cases, the DIO may hold a meeting with the relevant staff to go through the request.

Appendix 4: Review of Information Guidelines

The DIO, if requested to do so, will provide advice and guidance as to whether any information may be subject to an exemption and/or if consent is required to be provided from a third party. It may also be necessary to redact aspects of documents identified, particularly if there is third party data.

The following guidelines are intended to provide assistance when reviewing a request, but are no substitute for a case by case analysis of the request:-

- Check that the record is actually about the person concerned and not about someone else with the same name.

- Screen out any duplicate records. For example, if there has been an e-mail exchange with some colleagues, the Council only needs to print out the last e-mail in the exchange if copies of all the other e-mails are part of the last e-mail.

- The Council should only disclose information which is about the person making the subject access request. Where a document contains personal data about other individuals, including the data subject, the Council should not disclose information about the third parties to the data subject. If the record is primarily about the data subject, with incidental information about others, then redactions should be applied to the third-party information. If the record is primarily about third parties, this may be withheld if redacting is not possible. Alternatively, the third party may be contacted to obtain consent to disclose the document.

- The records may contain correspondence and comments about the data subject from a number of parties, including private individuals, external individuals acting in an official capacity, and our staff. In these cases, we are required to balance the interests of the third party against the interests of the data subject and often omit or redact third party information.

- The Council will not disclose information which would prejudice the prevention or detection of a crime. For example, if the Police inform the Council that a member of staff is under investigation, but the member of staff did not know this, then we will not provide that information to the member of staff whilst the investigation is in progress. However, if the investigation is closed or if the member of staff has been informed that there is an investigation underway, then the information may be disclosed in response to a subject access request.

- Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six-month period of the original request will be considered a repeat request, and the Council will not normally provide a further copy of the same data.

- The Council will not provide copies of documents which are already in the public domain.

- Any privileged information held by the Council need not be disclosed in response to a SAR. In general, privileged information includes any document which is direct communication between a client and his/her lawyer and is created for the purpose of obtaining or giving legal advice.

The above guidelines are not exhaustive and the DIO should be contacted for specific advice.

The process may discover material which does not reflect favourably on the Council. For example, documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject. These documents must be disclosed unless an exemption applies.

Appendix 5: Response Guidelines

The DIO, where requested, will provide a template response letter to the Council who will then send the response to the requester on its Council letterhead. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The Council will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

When responding to the request, information about how to make a complaint to the Council, or the Information Commissioner's Office, will be provided.

This page is intentionally left blank.

DATA BREACH PROCEDURE

Hertford Town Council

Adopted June 2023

Review June 2025

Policy Statement

1.1 Hertford Town Council ("the Council") processes personal information (electronic or paper based) about individuals in order to provide services to people within our community. It is also necessary to process personal information about our staff and others who we come into contact with during the course of our operations. This can include sensitive information ("Special Category Data") such as health data.

1.2 By complying with our own internal data protection procedures, and through promoting a strong culture of data protection compliance, our aim is to avoid the occurrence of a data breach. However, we recognise that in the event of a data breach, it is critical that we have effective response procedures in place to minimise the impact on those affected.

1.3 This policy applies to all Council staff (including employees, officers, workers and consultants). This policy does not form part of any contract of employment and may be amended at any time.

Data Breach

2.1 A data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. It is therefore important to recognise that a data breach is not just the loss of personal information.

2.2 Examples of data breaches include the following:

(a) Loss or theft of personal data and / or equipment on which data is stored
(b) Sending personal information to the incorrect recipient
(c) Unauthorised access of personal information
(d) Hacking
(e) Cyber-attack
(f) Accidental destruction

2.3 The above list is not exhaustive. If you are in any doubt as to whether a data breach has occurred or not, you should err on the side of caution and report it in accordance with this procedure.

Reporting a data breach

Any person who has personally caused a data breach, discovers a data breach, or is informed of the occurrence of a data breach, must immediately notify the Data Information Officer ("DIO"), HY Solicitors, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL by email to dpo@wearehy.com or by telephoning 0161 8041144.

PROCESS

Our response to any reported data security breach will involve the following steps:-

1. Report
2. Containment and Recovery
3. Assessment of Risks
4. Consideration of Further Notification
5. Evaluation and Response

Guidelines for each step are outlined in appendices 1 to 5

Appendix 1: Report

On receipt of the report, the DIO will obtain and record the initial details of the breach in the Data Breach Record.

Appendix 2: Containment and recovery guidelines

1. The DIO will determine if the breach is still occurring. If so, appropriate steps will be taken immediately to minimise the effect of the breach.
2. An initial assessment will be made by the DIO to establish the severity of the breach and to decide who will take the lead investigating the breach (this will depend on the nature of the breach; in most cases this will be the DIO).
3. Steps will be taken to establish who may need to be notified as part of the initial containment.
4. The DIO, in liaison with relevant staff, will determine the suitable course of action to be taken to ensure a resolution to the incident.

Appendix 3: Assessment of Risks guidelines

1. An investigation will be undertaken by the DIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.
2. The DIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.
3. The investigation will need to take account of the following:
    a. the type of data involved
    b. its sensitivity
    c. the protections in place (e.g. encryptions)
    d. what has happened to the data (e.g. has it been lost or stolen)
    e. whether the data could be put to any illegal or inappropriate use
    f. data subject(s) affected by the breach
    g. number of individuals involved and the potential effects on those data subject(s)
    h. whether there are wider consequences to the breach

Appendix 4: Consideration of Further Notification guidelines

1. The DIO will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify within 72 hours of becoming aware of the breach.
2. Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:
    a. whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation
    b. whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?)
    c. whether notification would help prevent the unauthorised or unlawful use of personal data

3. Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay.

    Notification will include:
    a. A description of how and when the breach occurred, and the data involved
    b. Specific and clear advice will be given on what they can do to protect themselves
    c. What action has already been taken to mitigate the risks
    d. A way in which they can contact us for further information or to ask questions on what has occurred

4. The DIO must consider advising the Council as to whether it is necessary to notify third parties such as the police, insurers, banks or credit and card companies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5. The DIO will consider whether a press release should be prepared.

6. All personal data breaches, regardless of whether notification was required, will be recorded in the data breach record.

Appendix 5: Evaluation and response guidelines

1. Once the incident has been addressed to its conclusion, and if the DIO deems it necessary, a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures is required will be undertaken.

Retention Policy & Schedule

Hertford Town Council

Adopted June 2023

Review June 2025

CONTENTS

1. About This Policy and Scope

1.1 This is the Retention Policy of Hertford Town Council ("the Council"). This policy sets out our approach to data retention and the retention periods which apply to different categories of data. It applies to both pesonal and non-personal data.

1.2 There are legal and regulatory requirements for us to retain certain data, usually for a specified amount of time. For other categories of data where there is not a specified period of time, the Council has determined the retention period by considering how long it is necessary for us to hold that data having regard to established legal principles.

1.3 This policy covers paper based records such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings.

1.4 This policy covers data that is held by third parties on our behalf, for example cloud storage providers.

1.5 This policy applies to all staff (including employees, officers, workers, and consultants). This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Guiding Principles

2.1 Through this policy, and our data retention practices, we aim to meet the following commitments:

- We comply with legal and regulatory requirements to retain data.
- We comply with our data protection obligations, in particular to keep personal data no longer than is necessary for the purposes for which it is processed (storage limitation principle).
- We handle, store and dispose of data responsibly and securely.
- We create and retain data where we need this to operate our function effectively, but we do not create or retain data without good business reason.
- We allocate appropriate resources, roles and responsibilities to data retention.
- We regularly remind employees of their data retention responsibilities.

3. Roles and Responsibilities

3.1 **Responsibility of all employees.** Good data management practices necessitate that all employees support the Council to retain data in accordance with this Policy. All employees must comply with this policy. An employee's failure to comply with this policy may result in disciplinary action. It is therefore the responsibility of everyone to understand and comply with this policy.

3.2 **Records Management.** We have designated the Civic Admistration Manager as the Records Management Officer. The Records Management Officer is responsible for administering this policy

3.3 **Data Information Officer**. Our Data Information Officer (DIO) is responsible for advising the Council on its records retention obligations.

4. Retention Periods

4.1 To assist the Council to meet its objectives set out at paragrah 2 (Guiding Principles), we have set out specific retention periods for the different categories of data which we process. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason calls for its continued retention.

4.2 Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (principle of storage limitation). Where data is listed in the Record Retention Schedule, we have taken into account the principle of storage limitation and balanced this against our requirements to retain the data.

4.3 If data is not listed in the Record Retention Schedule, or you are unsure whether to retain a certain record, please contact the Records Management Officer for guidance.

5. Storage, Back-Up And Disposal Of Data

5.1 **Storage.** Our data must be stored in a safe, secure, and accessible manner.

5.2 **Destruction**. Our Records Management Officer is responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with the support of those responsible for IT functions.

Hertford Town Council

Council Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Council Minutes	Indefinite	Best practice	Council meeting minutes should be retained for archiving in the public interest
Meeting Agendas	Date of meeting + 10 years	Best practice	
Play area equipment inspection records	Date created + 21 years	Business need	

Financial Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Scales of fees and charges	Date superseded + 6 years	Best practice	
Cheque book stubs	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
Receipt and payment accounts	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
Receipts	Financial year + 6 years	Tax, VAT, Limitation Act 1980	

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Paid invoices	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
VAT records	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
Petty cash records	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
Members Allowances register	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
Lettings diaries	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
Applications to hire halls, centres, or recreation grounds	Financial year + 6 years	Tax, VAT, Limitation Act 1980	
All records relating to burial grounds (e.g. register of fees collected, register of burials, register of purchased graves)	Indefinite	Local Authorities Cemeteries Order 1977 (SI 204)	

HR Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Recruitment records These may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) Criminal records checks. (These may be transferred to a	6 months after notifying candidates of the outcome of the recruitment exercise.		

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
successful candidate's employment file if they are relevant to the ongoing relationship.)			
Immigration checks			
	Three years after the termination of employment.		
Contracts			
These may include: Written particulars of employment. Contracts of employment or other contracts. Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.		
Collective agreements			
Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues		

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
	and for seven years after employment ends.		
Payroll and wage records			
Payroll and wage records Details on overtime. Bonuses. Expenses. Benefits in kind.	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.		
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made		
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be		

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
	retained for seven years after employment ends.		
Payroll and wage records for companies	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.		
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.		

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Travel and subsistence.	While employment continues and for seven years after employment ends.		
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.		
Personnel records			
These include: Qualifications/references. Consents for the processing of special categories of personal data. Annual leave records. Annual assessment reports. Disciplinary procedures. Grievance procedures. Death benefit nomination and revocation forms. Resignation, termination and retirement.	While employment continues and for seven years after employment ends.		
Records in connection with working time			

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Working time opt-out	Three years from the date on which they were entered into.		
Records to show compliance, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.		
Maternity records			
These include: Maternity payments. Dates of maternity leave. Period without maternity payment. Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.		
Accident records			
These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made		

Pensions Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Name and address of scheme or provider of the automatic enrolment scheme used to comply with the employer's duties.	6 years	Employers' Duties (Registration and Compliance) Regulations 2010 (*SI 2010/5*) (Employers' Duties Regulations 2010) (regulations 5, 6 and 8).	Minimum statutory period.
Employer pension scheme reference.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Evidence scheme complies with auto-enrolment statutory quality tests.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Name, NI number, date of birth and automatic enrolment date of all jobholders auto-enrolled (and corresponding details for non-eligible jobholders and entitled workers who have opted in or joined).	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Evidence of jobholders' earnings and contributions.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Contributions payable by employer in respect of jobholders and dates on which employer contributions were paid to scheme.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
If auto-enrolment postponement period used, records of workers who were given notice of postponement including full name, NI number and date postponement notice was given.	6 years	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period.
Auto-enrolment opt-in notices, joining notices and opt-out notices (original format).	6 years (4 years for opt-out notices)	Employers' Duties Regulations 2010 (regulations 5, 6 and 8).	Minimum statutory period. Opt-in notices, joining notices and opt-out notices must be kept in the original format, although copies of the original format or electronically stored versions are acceptable (*Pensions Regulator, Detailed Guidance Note 9, Keeping records, paragraph 8*).
If the Council is (or was) sponsoring employer of an occupational pension scheme,	For the tax year to which they relate and the following 6 years	Registered Pension Schemes (Provision of Information) Regulations	Minimum statutory period.

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
any document relating to monies received by or owing to the scheme, investments or assets held by the scheme, payments made by the scheme, contracts to purchase a lifetime annuity in respect of scheme member and documents relating to the administration of the scheme.		2006 (*SI 2006/567*) (regulation 18).	
Information relating to applications for ill health early retirement benefits, including medical reports.	While entitlement continues and for period of 15 years after benefits stop being paid.	Limitation period	Employers may also need to keep data relating to employees' job descriptions to assist with any ill-health application.
Death benefit nomination and revocation forms.	While entitlement continues and for period of 15 years after the death of member and their beneficiaries.	Limitation period	Longer may be required for public sector employees e.g. the National Archives suggests 100 years from date of birth.

Planning Papers

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Applications	Final decision for application + 1 year	Best practice	

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Appeals	Final decision for application + 1 year	Best practice	
Local Development Plans	6 years from being superseded	Business need	
Local Plans	6 years from being superseded	Business need	
Town and Neighbourhood Plans	Indefinite	Archive purposes	

Facilities and Security Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
CCTV recordings.	90 days for routine recordings As long as necessary for any investigations or claims that arise	Best practice	No set period in law but as these can contain personal data, should be kept for no longer than is necessary for the purpose. Relevant authorities must comply with the Surveillance Camera Code of Practice.
Visitor logs.	6 months	Best practice	No set period in law but as these can contain personal data, should be kept for no longer than is necessary for the purpose.

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Property management and asset records.	6 years or 12 years depending on whether the agreement is executed as a simple contract or a deed respectively	Limitation period	If agreement has been executed as a simple contract, actions are time barred 6 years from the date of breach of contract (*section 5, Limitation Act 1980*). If the agreement is executed as a deed, actions are time barred 12 years from the accrual of the cause of action (*section 8, Limitation Act 1980*).
Building contracts.	12 years from practical completion when executed as a deed	Limitation period	An organisation may wish to break this down into sub-categories of agreement, for example, professional appointment, building contract, collateral warranty, third-party rights, development agreement and novation or assignment documents. An organisation may also wish to list related documents such as insurance and finance, for example, bonds and parent company guarantees. In addition, consideration should be given to other records relating to the building works, such as correspondence, which may be required in the event of a dispute.
Leases.	6 or 12 years depending on the issue	Limitation period	If the tenant has not paid rent, the landlord is time barred from recovering the same 6 years from the date the rent became due (*section 19, LA 1980*). Otherwise because a lease is usually

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
			executed as a deed, actions under leases are time barred 12 years from the accrual of the cause of action (section 8, LA 1980).
Health and safety files for building works.	6 years from completion	Limitation period	Organisations may wish to retain for longer to assist with future works and maintenance.

IT Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
General information about internally developed IT infrastructure, software and systems for internal use.	5 years from decommissioning of system	Business need	No statutory period so organisation can balance need to retain these records against data minimisation principle.
General information about externally developed IT infrastructure, software and systems for internal or external use.	7 years from decommissioning of system	Contractual obligation Limitation period	See also Procurement section
General information about internally developed IT infrastructure, software and systems for external use.	7 years from decommissioning of system	Contractual obligation Limitation period	Where IT infrastructure, software or systems are used externally (for example, by customers) then this information may be relevant to claims and disputes.

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Systems monitoring, (for example, to detect and prevent failures vulnerabilities and external threats).	Current year plus 1 year Consider whether records can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these logs for longer or indefinitely	Business need Contractual obligation Limitation period	No statutory period so organisation can balance need to retain these records against data minimisation principle. It may be advisable for an organisation to keep monitoring logs for as long as possible as malware or malicious code may go undetected in a system for a long period of time. Where IT infrastructure, software or systems are used externally (for example, by customers), monitoring logs might also be relevant to claims and disputes.
Business continuity and information security plans.	3 years from when the plan is superseded Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a contractual or legal obligation to keep these plans for a longer period.	Business need Legal or contractual obligation Limitation period	No statutory period so organisation can balance need to retain these records against data minimisation principle. However, consider whether organisation is subject to any legal or contractual obligations in respect of business continuity which might necessitate a longer retention period, for example, under the NIS Regs. Where IT infrastructure, software or systems are used externally (for example, by customers), business continuity plans might also be relevant to claims and disputes.

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Technical support and help-desk requests.	3 years from end of system Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these requests for a longer period (for example, 7 years to align with limitation periods)	Business need. Contractual obligation. Limitation period.	No statutory period so organisation can balance need to retain these records against data minimisation principle. Consider whether support services are provided to external customers, in which case contractual obligations and limitation periods may be relevant.
Technical information relating to external customer user accounts.	1 year from account closure. Consider whether record can be fully anonymised after this period (or no personal data collected in first place) where there is a need to keep these plans for a longer period.	Business need Contractual obligation Limitation period	No statutory period so organisation can balance need to retain these records against data minimisation principle. Consider whether contractual obligations and limitation periods may be relevant.
Contracts and agreements (software licences, support	7 years from expiry of the agreement	Limitation period	See also Procurement section.

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
agreements, hardware agreements etc.).			
System backups.	3 months	Business need	May be different depending on the system.

Procurement Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Unsuccessful tenders	2 years	Business need	Businesses that have a large number of tenders may prefer to only retain for 1 year but will depend on the nature of the business.
Successful tenders	Contract period plus 6 years (12 years for contracts executed as a deed).	Limitation period	
Contractual documents	Contract period plus 6 years (12 years for contracts executed as a deed).	Limitation period	

Legal Records

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Legal advice and opinions (non-litigation).	6 years after life of the service or matter the advice relates to	Business need and limitation period in the event of a related claim	
Legal advice and other records relating to specific litigation or claim.	6 years from settlement or withdrawal of claim	Limitation period	
Data subject rights requests	6 years from closure of request	Limitation period	
Previous versions of policies, including IT policy, privacy policy, retention policy etc.	6 years form being superseded	Business need and limitation period in the event of a related claim	
Monitoring and investigation requests	6 years from closure of investigation	Limitation period	
Insurance claims	3 years after settlement	Limitation period	

This page is intentionally left blank.

Appendix 4a

Document 6.16

RETENTION AND DISPOSAL OF DATA POLICY

(Guidance for Councillors and Officers)

Adopted 8 May 2018
Review by June 2023

1. Introduction

1.1 The Council accumulates information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of document.

1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.

1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.

1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the Council.

1.5 The Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations ('the Regulations') so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

2. Scope and Objectives of the Policy

2.1 The aim of this document is to provide a working framework to determine which documents are:

2.1.1 retained – and for how long; or

2.1.2 disposed of – and if so by what method.

2.2 There is some information that does not need to be kept at all or that are routinely destroyed in the course of daily business. This usually applies to information that is duplicated, unimportant or only of a short-term value. This may include:

2.2.1 'With compliments' slips;

2.2.2 non-acceptance of invitations;

2.2.3 electronic mail messages that are not related to Council business;

2.2.4 requests for information such as maps, plans or advertising material.

2.3 Records should not be destroyed if the information can be used as evidence to prove that something has happened. If destroyed the disposal needs to be disposed of under the Regulations.

3. Roles and Responsibilities for Document Retention and Disposal

3.1 The Council is responsible for determining whether to retain or dispose of documents and will undertake a review of documentation at least on an annual basis to ensure that any unnecessary documentation being held is disposed of under the Regulations.

3.2 The Council ensures that all employees are aware of the retention/disposal schedule.

4. Document Retention Protocol

4.1 The Council has in place an adequate system for documenting the activities of the service. This system takes into account the legislative and regulatory environments to which it works.

4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:

4.2.1 facilitate an audit or examination of the business by anyone so authorised;

4.2.2 protect the legal and other rights of the Council, its clients and any other persons affected by its actions;

4.2.3 verify individual consent to record, manage and record disposal of their personal data;

4.2.4 provide authenticity of the records so that the evidence derived from them

is shown to be credible and authoritative.

4.3 To facilitate this the following principles should be adopted:

4.3.1 records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the Regulations;

4.3.2 documents that are no longer required for operational purposes but need retaining should be placed at the records office.

4.4 The retention schedules in 'Appendix A: List of Documents for Retention or Disposal' provide guidance on the recommended minimum retention periods for specific classes of documents and records. These schedules have been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.

4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

5. Document Disposal Protocol

5.1 Documents should be disposed of once they have been reviewed in accordance with the following:

5.1.1 is retention required to fulfil statutory or other regulatory requirements?

5.1.2 is retention required to meet the operational needs of the service?

5.1.3 is retention required to evidence events in the case of dispute?

5.1.4 is retention required because the document or record is of historic interest or intrinsic value?

5.2 When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the Regulations.

5.3 Documents can be disposed of by any of the following methods:

5.3.1 Non-confidential records: placed in the recycling bin for disposal;

5.3.2 confidential records or records giving personal information: shred documents and thereafter dispose of using appointed contractor;

5.3.3 deletion of computer records including those in the recycle bin;

5.3.4 transmission of records to an external body such as the County Records Office.

5.4 The following principles should be followed when disposing of records:

5.4.1 all records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the Council being prosecuted under the Regulations and or cause reputational damage;

5.4.2 the Freedom of Information Act and any other regulations; codes of practice and guidance issued;

where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner;

5.4.3 where documents are of historical interest it may be appropriate that they are transmitted to the County Records office;

5.4.4 back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).

6. List of Documents

6.1 The full list of the Council's documents and the procedures for retention or disposal can be found in Appendix A: List of Documents for Retention and Disposal. This is updated regularly in accordance with any changes to legal requirements.

This page is intentionally left blank.

PUBLIC PRIVACY POLICY

WHAT IS THE PURPOSE OF THIS POLICY?

Hertford Town Council ("the Council") is committed to protecting the privacy and security of your personal information.

This privacy policy describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR").

The Council is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy policy.

This policy applies to all individuals who engage in services with the Council. This policy does not form part of any contract to provide services. We may update this policy at any time but if we do so, we will provide you with an updated copy of this policy as soon as reasonably practical.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified.

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Address
- Gender
- CCTV footage and other information obtained through electronic means
- Photographs

We may also collect, store and use the following “special categories” of more sensitive personal information:

- [Information about your health, including any medical condition, health and sickness records
- Ethnic group
- Race
- Religion
- Trade union membership
- Sexuality
- Biometric data
- Information about criminal convictions and offences]

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about you if you subscribe to or apply for services that require personal information.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform or manage the services you have requested;
- Where we need to prevent and detect fraud and corruption in the use of public funds;
- Where it is necessary to meet our statutory obligations; or
- Where it is necessary in the exercise of our official authority or to perform a task in the public interest that is set out in law.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- In circumstances where we need your consent.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to provide services to you and to enable us to comply with legal obligations. The situations in which may process your personal information include the following:-

- to perform the service you requested, and to monitor and improve the Council's performance in responding to your request;
- to allow us to be able to communicate and provide services and benefits appropriate to your needs;
- to ensure that we meet our legal obligations;
- to prevent and detect fraud or crime.
- to process relevant financial transactions, including grants and payments for goods and services supplied to the Council;
- to allow the statistical analysis of data so we can plan the provision of services.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to provide the service you have requested, or we may be prevented from complying with our legal obligations (such as ensuring the health and safety of individuals on our premises).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the

original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- With your explicit consent.
- Where there is a substantial public interest condition that we can rely on.

Our obligations

We will use your particularly sensitive personal information in the following ways:

- We will use information about your physical or mental health, or disability status, to ensure your health and safety while accessing services provided by the Council.

DATA SHARING

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law or where it is necessary to administer the services to you.

DATA SECURITY

We have put in place measures to protect the security of your information.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those staff, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Once you are no longer an employee, worker or contractor of the Council we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Should you wish to obtain more specific information about how long we hold different categories of your personal information for, please contact the DIO.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information in certain circumstances.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DIO.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

DATA INFORMATION OFFICER

We have appointed a DIO, HY Solicitors, to oversee compliance with this privacy policy. If you have any questions about this privacy policy or how we handle your personal information, please contact the DIO by emailing dpo@wearehy.com. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to update this privacy policy at any time, and we will provide you with a new privacy policy when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Hertford Town Council

What is the Purpose of this Privacy Notice

Welcome to Hertford Town Council's privacy notice.

Hertford Town Council respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you contact and/ or visit the Council and our website (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The GDPR and DPA contain key laws relating to data protection.

We process and hold information in order to provide public services. This notice explains how we use and share your information. Information may be collected on paper or online form, by telephone, email or by a member of our staff, or one of our partners.

The Data Information Officer

We have appointed a Data Information Officer (DIO), HY Professional Services, who can be contacted in writing at HY Professional Services, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL or by telephone on 0161 804 1144. The DIO is responsible for dealing with data protection issues within the Council and you can contact the DIO should you wish to discuss any issues or concerns that you have about this privacy policy or our privacy practices.

The Data we collect about You

- Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).
- address
- date of birth

Some types of information are regarded as more sensitive under the GDPR and referred to as being a 'special category' of personal information and is likely to include anything that can reveal your:

- criminal history
- ethnicity
- genetic or biometric data
- physical or mental health

- political opinion
- religious or philosophical beliefs
- sexuality
- sexual health
- trade union membership

How is Your Personal Data collected

We record personal information if you:

- directly interact with us and provide us with your personal information;
- subscribe to or apply for services that require personal information;
- report a fault and give your contact details for us to respond;
- give us feedback or contact us and leave your details for us to respond;
- enter a competition, promotion or survey.

Why we collect information

We collect and hold information about you, in order to:

- confirm your identity to provide services and support to you;
- manage the services we provide to you;
- contact you by post, email or telephone;
- understand your needs to provide the services that you request;
- understand what we can do for you and inform you of other relevant services and benefits;
- obtain your opinion about our services;
- help investigate any worries or complaints you have about the services you receive;
- update your customer record;
- help us to build up a picture of how we are performing at delivering services;
- prevent and detect fraud and corruption in the use of public funds;
- allow us to undertake statutory functions efficiently and effectively;
- make sure we meet our statutory obligations.

We will process your information for the following purposes:

- for the service you requested, and to monitor and improve the council's performance in responding to your request.
- to allow us to be able to communicate and provide services and benefits appropriate to your needs.
- to ensure that we meet our legal obligations.
- where necessary for the law enforcement functions.
- to prevent and detect fraud or crime.

- to process relevant financial transactions including grants and payments for goods and services supplied to the Council.
- where necessary to protect individuals from harm or injury.
- to allow the statistical analysis of data so we can plan the provision of services.

Our Right to Process Information

We are subject to a wide range of laws which we must comply with to deliver our services to you. To comply with these laws, we only process personal information as far as is necessary to meet those obligations. We process some of the information described in this privacy notice to carry out a:

- public tasks
- legal obligation
- contractual obligation
- vital interest.

In the absence of any other lawful ground for processing, we will obtain your consent.

Sharing Your Personal Information

We may need to pass your information to other people and organisations that we have contracted with or partnered with in order to provide any of the services that you receive. These providers are obliged to keep your details securely and use them only to fulfil your request.

Information Security

Hertford Town Council cares to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted.

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Your Rights
Access to Information

You have the right to request access to the information we have about you. You can do this by contacting our Data Information Officer: DPO@wearehy.com

Information Correction

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: DPO@wearehy.com

Information Deletion

If you wish Hertford Town Council to delete the information about you please contact: DPO@wearehy.com

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact DPO@wearehy.com

Rights Related to Automated Decision Making and Profiling

Hertford Town Council does not use automated decision making or profiling of individual personal data.

To Sum Up

In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell your data. We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We constantly review our Privacy Policies to keep it up to date in protecting your data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to Hertford Town Council Data Information Officer: DPO@wearehy.com and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

HY (DIO for Hertford Council)
Reed House
Hunters Lane
Rochdale
Greater Manchester
DPO@wearehy.com
0161 804 1144

HERTFORD TOWN COUNCIL

Hirers Privacy Notice – Castle and Mill Bridge Room

What is the Purpose of this Privacy Notice

Welcome to Hertford Town Council's privacy notice in relation to the Castle and Mill Bridge Room.

Hertford Town Council respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our website and/ or the Council and enquire about or hire the Castle or Mill Bridge room and tell you about your privacy rights and how the law protects you under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The GDPR and DPA contain key laws relating to data protection.

When you hire the Castle or Mill Bridge room the information you provide (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible to contact you and respond to your correspondence, provide information, send invoices and receipts relating to your hire agreement.

This notice explains how we use and share your information. Information may be collected on paper or online form, by telephone, email or by a member of our staff, or one of our contracted partners.

The Data InformationOfficer

We have appointed a Data Information Officer (DIO), HY Professional Services, who can be contacted in writing at HY Professional Services, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL or by telephone on 0161 804 1144. The DIO is responsible for dealing with data protection issues within the Council and you can contact the DIO should you wish to discuss any issues or concerns that you have about this privacy policy or our privacy practices.

The Data we collect about You

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

- name
- address
- date of birth

Some types of information are regarded as more sensitive under the GDPR and referred to as being a 'special category' of personal information and is likely to include anything that can reveal your:

- criminal history
- ethnicity
- genetic or biometric data
- physical or mental health
- political opinion
- religious or philosophical beliefs
- sexuality
- sexual health
- trade union membership

How is Your Personal Data collected

We record personal information if you:

- directly interact with us and provide us with your personal information;
- subscribe to or apply for services that require personal information;
- give us feedback or contact us and leave your details for us to respond;
- enter a competition, promotion or survey.

Why we collect information

We collect and hold information about you, in order to process your enquiry or room hire.

We will process your information for the following purposes:

- for the service you requested, and to monitor and improve the council's performance in responding to your request;
- to ensure that we meet our legal obligations, if a contract is entered into;
- where necessary for the law enforcement functions;
- to prevent and detect fraud or crime;
- to process relevant financial transactions including grants and payments for goods and services supplied to the Council;
- where necessary to protect individuals from harm or injury;
- to allow the statistical analysis of data so we can plan the provision of services.

Our Right to Process Information

We are subject to a wide range of laws which we must comply with to deliver our services to you. To comply with these laws, we only process personal information as far as is necessary to meet those obligations.

Sharing Your Personal Information

We may need to pass your information to other people and organisations that we have contracted with or partnered with in order to provide any of the services that you receive. These providers are obliged to keep your details securely and use them only to fulfil your request.

Information Security

Hertford Town Council cares to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted.

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Your Rights
Access to Information

You have the right to request access to the information we have about you. You can do this by contacting our Data Information Officer: town.clerk@hertford.gov.uk

Information Correction

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: town.clerk@hertford.gov.uk

Information Deletion

If you wish Hertford Town Council to delete the information about you please contact: town.clerk@hertford.gov.uk

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact town.clerk@hertford.gov.uk

Rights Related to Automated Decision Making and Profiling

Hertford Town Council does not use automated decision making or profiling of individual personal data.

To Sum Up

In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell your data. We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We constantly review our Privacy Policies to keep it up to date in protecting your data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to Hertford Town Council Data Information Officer: DPO@wearehy.com and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

HY (DIO for Hertford Council)
Reed House
Hunters Lane
Rochdale
Greater Manchester
DPO@wearehy.com
0161 804 1144

HERTFORD TOWN COUNCIL

General Data Protection Regulations Allotment Tenants Privacy Notice

To be signed and returned with your Allotment Tenancy Agreement.

Hertford Town Council respects your privacy and is committed to protecting your personal data. The attached privacy policy will inform you as to how we look after your personal data when you enter into an Allotment Tenancy Agreement. The information you provide (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible to contact you and to respond to your correspondence, provide information, send invoices and receipts relating to your allotment.

We process and hold information in order to provide public services. The attached notice explains how we use and share your information. Information may be collected on paper or online form, by telephone, email or by a member of our staff, or one of our partners.

Consent for your personal information to be held

I agree that I have read and understand Hertford Town Council Privacy Notice (attached). I agree by signing below that the Council may process my personal information for providing information and corresponding with me.

I agree that Hertford Town Council can keep my contact information data for no longer than is necessary.

I have the right to request modification on the information that you keep on record.

Name	
Date of birth	
Address	
Telephone No.	
Email Address	
Facebook	
Twitter	

Signature	
Date	

For office use only:

Guidance Notes Data Sharing Checklist – systematic data sharing
Scenario: You want to enter into an agreement to share personal data on an ongoing basis is this form relevant and the sharing justified? Read the below:

Key points to consider:
What is the sharing meant to achieve?
Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place.
As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared?
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Date Data received	Date consent received and approved for data to be held	Data received as Phone, email, hard copy or other	Data approved to be shared with the below	Removal of consent received	Date data disposed of and method of disposal actioned

HERTFORD TOWN COUNCIL

Purchase of Exclusive Rights of Burial Consent Form

Hertford Town Council respects your privacy and is committed to protecting your personal data. The attached privacy policy will inform you as to how we look after your personal data when you purchase the Exclusive Right to a single or joint cemetery plot. The information you provide (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible to contact you and to respond to your correspondence, provide information, send invoices and receipts relating to your burial plot/s.

We process and hold information in order to provide public services. The attached notice explains how we use and share your information. Information may be collected on paper or online form, by telephone, email or by a member of our staff, or one of our partners.

Consent for your personal information to be held

I agree that I have read and understand Hertford Town Council's Privacy Notice (attached). I agree by signing below that the Council may process my personal information for providing information and corresponding with me.

I agree that Hertford Town Council can keep my contact information data for no longer than is necessary.

I have the right to request modification on the information that you keep on record.

Name	
Date of birth	
Address	
Telephone No.	
Email Address	
Facebook	
Twitter	
Signature	
Date	

For office use only:

Guidance Notes Data Sharing Checklist – systematic data sharing
Scenario: You want to enter into an agreement to share personal data on an ongoing basis is this form relevant and the sharing justified? Read the below:

Key points to consider:
What is the sharing meant to achieve?
Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place.
As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared?
- •The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Date Data received	Date consent received and approved for data to be held	Data received as Phone, email, hard copy or other	Data approved to be shared with the below	Removal of consent received	Date data disposed of and method of disposal actioned

HERTFORD TOWN COUNCIL

Neighbourhood Plan Privacy Notice

What is the Purpose of this Privacy Notice

Welcome to Hertford Town Council's privacy notice in relation to the Neighbourhood Plan.

Hertford Town Council respects your privacy and is committed to protecting your personal data. This privacy policy will inform you as to how we look after your personal data when you attend a consultation event or return a survey or consultation document, the information you provide (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible to contact you and respond to your correspondence and provide information relating to the Neighbourhood Plan. This notice will tell you about your privacy rights and how the law protects you under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The GDPR and DPA contain key laws relating to data protection.

This notice explains how we use and share your information. Information may be collected on paper or online form, by telephone, email or by a member of our staff, or one of our contracted partners.

The Data Information Officer

We have appointed a Data Information Officer (DIO), HY Professional Services, who can be contacted in writing at HY Professional Services, 1 Reed House, Hunters Lane, Rochdale, OL16 1YL or by telephone on 0161 804 1144. The DIO is responsible for dealing with data protection issues within the Council and you can contact the DIO should you wish to discuss any issues or concerns that you have about this privacy policy or our privacy practices.

The Data we collect about You

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

- name
- address

- date of birth

Some types of information are regarded as more sensitive under the GDPR and referred to as being a 'special category' of personal information and is likely to include anything that can reveal your:

- criminal history
- ethnicity
- genetic or biometric data
- physical or mental health
- political opinion
- religious or philosophical beliefs
- sexuality
- sexual health
- trade union membership

How is Your Personal Data collected

We record personal information if you:

- directly interact with us and provide us with your personal information;
- subscribe to or apply for services that require personal information;
- report a fault and give your contact details for us to respond;
- give us feedback or contact us and leave your details for us to respond;
- enter a competition, promotion or survey.

Why we collect information

We collect and hold information about you, in order to:

- confirm your identity to provide services and support to you;
- manage the services we provide to you;
- contact you by post, email or telephone;
- understand your needs to provide the services that you request;
- understand what we can do for you and inform you of other relevant services and benefits;
- obtain your opinion about our services;
- help investigate any worries or complaints you have about the services you receive;
- update your customer record;
- help us to build up a picture of how we are performing at delivering services;
- prevent and detect fraud and corruption in the use of public funds;

- allow us to undertake statutory functions efficiently and effectively;
- make sure we meet our statutory obligations.

We will process your information for the following purposes:

- for the service you requested, and to monitor and improve the council's performance in responding to your request.
- to allow us to be able to communicate and provide services and benefits appropriate to your needs.
- to ensure that we meet our legal obligations.
- where necessary for the law enforcement functions.
- to prevent and detect fraud or crime.
- To process relevant financial transactions including grants and payments for goods and services supplied to the Council
- where necessary to protect individuals from harm or injury.
- to allow the statistical analysis of data so we can plan the provision of services.

Our Right to Process Information

We are subject to a wide range of laws which we must comply with to deliver our services to you. To comply with these laws, we only process personal information as far as is necessary to meet those obligations.

Sharing Your Personal Information

We may need to pass your information to other people and organisations that we have contracted with or partnered with in order to provide any of the services that you receive. These providers are obliged to keep your details securely and use them only to fulfil your request.

Information Security

Hertford Town Council cares to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and appropriate policies. We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted.

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Your Rights

Access to Information

You have the right to request access to the information we have about you. You can do this by contacting our Data Information Officer: DPO@wearehy.com

Information Correction

If you believe that the information we have about you is incorrect, you may contact us so that we can update it and keep your data accurate. Please contact: DPO@wearehy.com

Information Deletion

If you wish Hertford Town Council to delete the information about you please contact: DPO@wearehy.com

Right to Object

If you believe that your data is not being processed for the purpose it has been collected for, you may object: Please contact DPO@wearehy.com

Rights Related to Automated Decision Making and Profiling

Hertford Town Council does not use automated decision making or profiling of individual personal data.

To Sum Up

In accordance with the law, we only collect a limited amount of information about you that is necessary for correspondence, information and service provision. We do not use profiling, we do not sell your data. We do not use your data for purposes other than those specified. We make sure your data is stored securely. We delete all information deemed to be no longer necessary. We constantly review our Privacy Policies to keep it up to date in protecting your data.

Complaints

If you have a complaint regarding the way your personal data has been processed you may make a complaint to Hertford Town Council Data Information Officer:DPO@wearehy.com and the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113

HY (DIO for Hertford Council)
Reed House
Hunters Lane
Rochdale
Greater Manchester

WORKFORCE PRIVACY POLICY

WHAT IS THE PURPOSE OF THIS POLICY?

Hertford Town Council ("the Council") is committed to protecting the privacy and security of your personal information.

This privacy policy describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (the retained EU law version of the General Data Protection Regulation (EU) 2016/679) ("GDPR").

It applies to all employees, officers, workers and contractors.

The Council is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy policy.

This policy applies to current and former staff (including employees, officers, workers, and consultants). This policy does not form part of any contract of employment or other contract to provide services. We may update this policy at any time but if we do so, we will provide you with an updated copy of this policy as soon as reasonably practical.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual, such as a staff member, from which that person can be identified.

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

We may collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Gender
- Marital or relationship status
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave and pension
- Start date and, if different, the date of your continuous employment
- Recruitment information (including copies of right to work documentation, references and other information included as part of the application process)
- Employment records (including job titles, work history, working hours, holidays, training records)
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as swipe card records
- Photographs

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your health, including any medical condition, health and sickness records
- Ethnic group

- Race
- Religion
- Trade union membership
- Biometric data
- Information about criminal convictions and offences

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you (e.g. using your bank details to ensure that you are paid).
- Where we need to comply with a legal obligation (e.g. making deductions for tax purposes).
- Where it is necessary in the exercise of our official authority or to perform a task in the public interest that is set out in law.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- In circumstances where we need your consent.

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. The situations in which may process your personal information include the following:-

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and

National Insurance contributions (NICs)

- Providing benefits
- Enrolling you in a pension arrangement
- Administering the contract we have entered into with you
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about your continued employment or engagement
- Gathering evidence for possible grievance or disciplinary or code of conduct hearings
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you), or we may be prevented from complying with our legal obligations (such as ensuring the health and safety of our staff).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leave, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay or statutory sick pay
- We will carry out criminal conviction (DBS) checks where the law requires us to do so

DATA SHARING

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law or where it is necessary to administer the working relationship with you.

Which third-party service providers process my personal information?

“Third parties” includes third-party service providers such as the local authority, pension administration or IT and telecoms providers.

DATA SECURITY

We have put in place measures to protect the security of your information.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, contractors and other third parties who have a

business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Once you are no longer an employee, worker or contractor of the Council we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Should you wish to obtain more specific information about how long we hold different categories of your personal information for, please contact the DIO.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information in certain circumstances.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DIO.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

DATA INFORMATION OFFICER

We have appointed a DIO, HY Solicitors, to oversee compliance with this privacy policy. If you have any questions about this privacy policy or how we handle your personal information, please contact the DIO by emailing dpo@wearehy.com. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to update this privacy policy at any time, and we will provide you with a new privacy policy when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

This page is intentionally left blank.

HERTFORD TOWN COUNCIL

PRIVACY NOTICE FOR STAFF, COUNCILLORS AND ROLE HOLDERS

***"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis**
****Includes volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.**

What is the purpose of this Notice?

This is Hertford Council's Privacy Notice which is intended to provide you with information about how and why we process your personal information. It is also intended to provide you with other information which is required under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The GDPR and DPA contain the key laws relating to data protection.

It is important to the Council, and a legal requirement, that we are transparent about how we process your personal information. As a Council that processes personal information, we are known as a "data controller". This means that we collect and use personal information for specified purposes which this Privacy Notice has been designed to tell you about.

The Data Protection Officer

The Council has appointed a Data Information Officer (DIO), HY Professional Services, who can be contacted by telephone on 0161 804 1144. The DIO is responsible for supporting and advising the Council in relation to data protection issues and you can contact the DIO should you wish to discuss any issues or concerns that you have about data protection.

What personal information do we collect?

The types of personal information that we collect will include:-

- personal information (such as name, employee number, national insurance number, next of kin and contact details)
- special categories of data including characteristics information (such as gender, age, ethnic group, race, and religion)
- photographs
- Recruitment information
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons, annual leave and maternity leave)
- qualifications, subjects taught and training records
- performance information
- grievance and disciplinary information
- health and safety information (such as accidents at work)
- relevant medical information
- safeguarding information
- DBS information
- CCTV footage and other information obtained through electronic means such as swipecard

records
- Right to work in the UK

What is the purpose of us collecting your personal information?
We process personal information relating to those we employ to work at, or otherwise engage to work at, the Council. This is for employment purposes to assist in the running of the Council and to enable individuals to be paid. The purposes for which we process workforce personal information include:-

- enabling the development of a comprehensive picture of the workforce and how it is deployed
- managing the recruitment process
- carrying out pre-employment checks and equal opportunities monitoring
- complying with the terms of the contract of employment
- making reasonable adjustments
- enabling individuals to be paid
- managing absence
- managing performance, grievance and disciplinary matters
- safeguarding purposes
- managing workplace accidents
- to administer Councilor's interests

Why is it lawful to collect this information?
Generally, we process your personal information, but no more so than is necessary, to comply with legal obligations which the Council is subject to or because processing is necessary to comply with the terms and conditions of your contract of employment.

In limited we circumstances, we may require your consent. If this is the case, we will inform you of the reasons that we need to process your personal information in accordance with the GDPR. You will be able to withdraw your consent at any time should you wish to do so.

Where we process sensitive personal information (special category data) we will usually do this, as far as necessary, to comply with employment law obligations which we are subject to or because it is in the public interest to do so.

Who will we share this information with?
We are required, by law, to pass on some of this personal information to the Monitoring Officer at East Hertfordshire District Council.

We also share information with bodies and/ organisations that may include:

- Health and Safety Executive
- HMRC
- DBS
- insurance providers
- training providers
- professional advisors
- former and prospective employers
- recruitment agencies;
- credit reference agencies
- staff pension providers
- DVLA

How long will we hold your information for?
We will hold personal information for a period of time specified within our retention policy. We generally hold staff personal information for the period of your employment until termination and a period of 6 years thereafter. For more information, please ask the Town Clerk for a copy of our retention schedule.

Requesting access to your personal data
Under data protection legislation, you have the right to request access to personal information that we hold about you. To make a request for your personal information please contact the Data Information Officer (DIO), HY Professional by email at DPO@wearehy.com or in writing:
HY (DIO for Hertford Council)
Reed House
Hunters Lane
Rochdale
Greater Manchester

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage or distress;
- Prevent processing for the purpose of direct marketing;
- Object to decisions being taken by automated means;
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection Regulations.

Complaints and further information

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

If you would like to discuss anything in this privacy notice, please contact the Data Information Officer (DIO), HY Professional Services at DPO@wearehy.com or in writing at:

HY (DIO for Hertford Council)
Reed House
Hunters Lane
Rochdale
Greater Manchester
DPO@wearehy.com
0161 804 1144