

# **General Data Protection Regulations (GDPR) Policies and Procedures**

Document includes:

1. Data Protection Policy
2. General Privacy Notice
3. Privacy Notice for Staff\*, Councillors and Role Holders\*\*
4. Privacy Policy
5. Subject Access Request Policy
6. Data Breach Policy
7. Document Retention Policy
8. Template Data Consent Form
9. Template GDPR Awareness Form

## **Document History**

Adopted by Council – 21<sup>st</sup> January  
2025 Next Review – 22<sup>nd</sup> January 2026



**Dawn Drury Town Clerk**

21/1/2025

**Chair of Council**



21/1/2025

# 1. Data Protection Policy

## 1. Introduction

- 1.1 The Town Council recognises its responsibility to comply with the General Data Protection Regulations (GDPR) 2018 and the Data Protection Act 2018 which regulate the use of personal data. The term is defined in Art. 4 (1). Personal data are any information which are related to an identified or identifiable natural person. Therefore, it can be as little as a name and address.

## 2. General Data Protection Regulations (GDPR)

- 2.1 The GDPR sets out high standards for the handling of personal information and protecting individuals' rights for privacy. It also regulates how personal information can be collected, handled and used.
- 2.2 The GDPR applies to anyone holding personal information about people, electronically or on paper. The Town Council has also notified the Information Commissioner that it holds personal data about individuals.
- 2.3 When dealing with personal data, Town Council staff and members must ensure that:
  - **Data is processed fairly, lawfully and in a transparent manner.** This means that personal information should only be collected from individuals if staff have been open and honest about why they want the personal information.
  - **Data is processed for specified purposes only.** This means that data is collected for specific, explicit and legitimate purposes only.
  - **Data is relevant to what it is needed for.** Data will be monitored so that too much or too little is not kept; only data that is needed should be held.
  - **Data is accurate and kept up to date and is not kept longer than it is needed.** Personal data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.
  - **Data is processed in accordance with the rights of individuals.** Individuals must be informed, upon request, of all the personal information held about them.
  - **Data is kept securely.** There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

## 3. Storing and accessing data

- 3.1 The Town Council recognises its responsibility to be open with people when taking personal details from them. This means that staff must be honest about why they want a particular piece of personal information.
- 3.2 The Town Council may hold personal information about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept at the Town Council Office and are not available for public access.
- 3.3 All data stored on the Town Council Office computers are password protected. Once data is not needed any more, is out of date or has served its use and falls

outside the minimum retention time of Councils document retention policy, it will be shredded or securely deleted from the computer.

- 3.4 The Town Council is aware that people have the right to access any personal information that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy, email or social media). If a person requests to see any data that is being held about them, the SAR response must detail:
  - How and to what purpose personal data is processed
  - The period the Town Council intends to process it for
  - Anyone who has access to the personal data
- 3.5 The response must be sent within 30 days and should be free of charge.
- 3.6 If a SAR includes personal data of other individuals, the Town Council must not disclose the personal information of the other individual. That individual's personal information may either be redacted, or the individual may be contacted to give permission for their information to be shared with the Subject.
- 3.7 Individuals have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing, although rules do apply to those requests.
- 3.8 Please see "Subject Access Request Procedure" for more details.

## **4. Confidentiality**

- 4.1 The Town Council members and staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives written permission otherwise. When handling personal data, this must also remain confidential

## 2. General Privacy Notice

### 1. Your personal data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

### 2. Who are we?

This Privacy Notice is provided to you by the **Keynsham Town Council** which is the data controller for your data.

Other data controllers the council works with:

- Keynsham Town Council
- Community groups
- Charities
- Other not for profit entities
- Contractors

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be “joint data controllers” which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

**The council will process some or all of the following personal data where necessary to perform its tasks:**

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

### **3. How we use sensitive personal data**

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

### **4. Do we need your consent to process your sensitive personal data?**

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full

details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

**The council will comply with data protection law. This says that the personal data we hold about you must be:**

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

## **5. We use your personal data for some or all of the following purposes:**

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;

- To process relevant financial transactions including grants and payments for goods and services supplied to the council, and;
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

## **6. What is the legal basis for processing your personal data?**

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

## **7. Sharing your personal data**

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

## **8. How long do we keep your personal data?**

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be

able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

## **9. Your rights and your personal data**

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

### **1) *The right to access personal data we hold on you***

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

### **2) *The right to correct and update the personal data we hold on you***

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

### **3) *The right to have your personal data erased***

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

### **4) *The right to object to processing of your personal data or to restrict it to certain purposes only***

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

### **5) *The right to data portability***

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

### **6) *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***



- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

**7) The right to lodge a complaint with the Information Commissioner's Office.**

- You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

## **10. Transfer of Data Abroad**

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

## **11. Further processing**

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

## **12. Changes to this notice**

We keep this Privacy Notice under regular review and we will place any updates on our website <http://www.keynsham-tc.gov.uk>

### **Contact Details**

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints to **The Data Controller**, in the following ways:

Address: **15-17 Temple Street, Keynsham, Bristol, BS31 1HF**

Telephone: **0117 986 8683**

Email: [townclerk@keynsham-tc.gov.uk](mailto:townclerk@keynsham-tc.gov.uk)

### **3. Privacy Notice for Staff\*, Councillors and Role Holders\*\***

\* "Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis.

\*\* "Role Holders" 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.

#### **Your personal data – what is it?**

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

#### **Who are we?**

This Privacy Notice is provided to you by **Keynsham Town Council** which is the data controller for your data.

#### **The council works together with:**

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration, then the data controllers will be independent and will be individually responsible to you.

#### **The council will comply with data protection law. This says that the personal data we hold about you must be:**

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

#### **What data do we process?**

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.

#### **We use your personal data for some or all of the following purposes: -**

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- 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, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract, we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

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

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

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

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

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

#### **How we use sensitive personal data**

- We may process sensitive personal data relating to staff, councillors and role holders including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

#### **Do we need your consent to process your sensitive personal data?**

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

### **Information about criminal convictions**

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.
- Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

### **What is the legal basis for processing your personal data?**

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

### **Sharing your personal data**

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions, or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

### **How long do we keep your personal data?**

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice

to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

### **Your responsibilities**

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

### **Your rights in connection with personal data**

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

#### **1. *The right to access personal data we hold on you***

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

#### **2. *The right to correct and update the personal data we hold on you***

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

#### **3. *The right to have your personal data erased***

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request, we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

#### **4. *The right to object to processing of your personal data or to restrict it to certain purposes only***

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request, we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

#### **5. *The right to data portability***

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.
- 6. *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***
- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).
- 7. *The right to lodge a complaint with the Information Commissioner's Office***
- You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

### **Transfer of Data Abroad**

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

### **Further processing**

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

### **Changes to this notice**

We keep this Privacy Notice under regular review and we will place any updates on our website <http://www.keynsham-tc.gov.uk>

### **Contact Details**

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints to **The Data Controller**, in the following ways:

Address: **15-17 Temple Street, Keynsham, Bristol, BS31 1HF**  
 Telephone: **0117 986 8683**  
 Email: [townclerk@keynsham-tc.gov.uk](mailto:townclerk@keynsham-tc.gov.uk)



## 4. Privacy Policy

### Your personal data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the “GDPR”) and other local legislation relating to personal data and rights such as the Human Rights Act.

### Council information

This Privacy Policy is provided to you by **Keynsham Town Council** which is the data controller for your data.

Address: **15-17 Temple Street, Keynsham, Bristol, BS31 1HF**

Telephone: **0117 986 8683**

Email: [townclerk@keynsham-tc.gov.uk](mailto:townclerk@keynsham-tc.gov.uk)

### Who are the data controllers?

- Keynsham Town Council
- Community groups
- Contractors

### What personal data is collected?

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process demographic information such as gender, age, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The data we process may include sensitive personal data or other special categories of data such as racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sex life or sexual orientation.
- Website data;
  - Information from syncing with other software or services
  - Interaction with social media
  - Information about payments
  - Access to social media profiles
  - Demographic information
- Information collected automatically from use of the service;
  - Device information (nature of device and/ or identifiers)
  - Log information (including IP address)
  - Location information

- Device sensor information
- Site visited before arriving
- Browser type and or OS
- Interaction with email messages
- Information from other sources;
  - Referral or recommendation programmes
  - Publicly accessible sources
- Information from cookies or similar technologies;
  - Essential login/authentication or navigation
  - Functionality – remember settings
  - Performance & Analytics – user behaviour
  - Advertising/retargeting
  - Any third-party software served on users
- Nature of any outbound communications with website users;
  - Email
  - Telephone (voice)

**The council will comply with data protection law. This says that the personal data we hold about you must be:**

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

**We use your personal data for some or all of the following purposes:**

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;

- To notify you of changes to our facilities, services, events and staff, councillors and role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council, and;
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

### **What is the legal basis for processing your personal data?**

The council is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometime when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Policy sets out your rights and the council's obligations to you in detail.

We may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

### **Sharing your personal data**

The council will implement appropriate security measures to protect your personal data. This section of the Privacy Policy provides information about the third parties with whom the council will share your personal data. These third parties also have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

### **How long do we keep your personal data?**

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

## **Your rights and your personal data**

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

- (i) The right to access personal data we hold on you*
- (ii) The right to correct and update the personal data we hold on you*
- (iii) The right to have your personal data erased*
- (iv) The right to object to processing of your personal data or to restrict it to certain purposes only*
- (v) The right to data portability*
- (vi) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained*
- (vii) The right to lodge a complaint with the Information Commissioner's Office.*

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

## **Transfer of Data Abroad**

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

## **Further processing**

If we wish to use your personal data for a new purpose, not covered by this Privacy Policy, then we will provide you with a Privacy Notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

## **Changes to this policy**

We keep this Privacy Policy under regular review and we will place any updates on our website <http://www.keynsham-tc.gov.uk>

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints to **The Data Controller**, in the following ways:

Address: **15-17 Temple Street, Keynsham, Bristol, BS31 1HF**

Telephone: **0117 986 8683**

Email: [townclerk@keynsham-tc.gov.uk](mailto:townclerk@keynsham-tc.gov.uk)

## 5. Subject Access Request Policy

### What must I do?

1. **MUST:** On receipt of a subject access request you must **forward** it immediately to the **Town Clerk who is the Data Controller**.
2. **MUST:** We must correctly **identify** whether a request has been made under the Data Protection legislation.
3. **MUST:** A member of staff, and as appropriate, councillor, who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive **search** of the records to which they have access.
4. **MUST:** All the personal data that has been requested must be **provided** unless an exemption can be applied.
5. **MUST:** We must **respond** within one calendar month after accepting the request as valid.
6. **MUST:** Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
7. **MUST:** Councillors and managers must ensure that the staff they manage are **aware** of and follow this guidance.
8. **MUST:** Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**.

### How must I do it?

1. Notify the **Town Clerk who is the Data Controller** upon receipt of a request.
2. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. You should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. The council accepts the following forms of identification (\* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):
  - Current UK/EEA Passport
  - UK Photocard Driving Licence (Full or Provisional)
  - Firearms Licence / Shotgun Certificate
  - EEA National Identity Card
  - Full UK Paper Driving Licence
  - State Benefits Entitlement Document\*
  - State Pension Entitlement Document\*
  - HMRC Tax Credit Document\*
  - Local Authority Benefit Document\*
  - State/Local Authority Educational Grant Document\*
  - HMRC Tax Notification Document
  - Disabled Driver's Pass
  - Financial Statement issued by bank, building society or credit card company+
  - Judiciary Document such as a Notice of Hearing, Summons or Court Order

- Utility bill for supply of gas, electric, water or telephone landline+
    - Most recent Mortgage Statement
    - Most recent council Tax Bill/Demand or Statement
    - Tenancy Agreement
  - Building Society Passbook which shows a transaction in the last 3 months and your address
3. Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.
  4. You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.
  5. Make this clear on forms and on the council website.
  6. You should do this through the use of induction, my performance and training, as well as through establishing and maintaining appropriate day to day working practices.
  7. A database is maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.
  8. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

#### Sample letters

#### **All letters must include the following information:**

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations,

including any appropriate safeguards for transfer of data, such as Binding Corporate Rules<sup>1</sup> or EU model clauses<sup>2</sup>;

- where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with the Information Commissioners Office (“ICO”);
- if the data has not been collected from the data subject: the source of such data;
- the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

### **Replying to a subject access request providing the requested personal data**

“[Name] [Address]

[Date]

Dear [Name of data subject]

#### **Data Protection subject access request**

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely”

### **Release of part of the personal data, when the remainder is covered by an exemption**

“[Name] [Address]

[Date]

Dear [Name of data subject]

#### **Data Protection subject access request**

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request, we asked the following areas to search their records for personal data relating to you:

---

<sup>1</sup> “Binding Corporate Rules” is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisation’s headquarters is located. In the UK, the relevant regulator is the Information Commissioner’s Office.

<sup>2</sup> “EU model clauses” are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely”

**Replying to a subject access request explaining why you cannot provide any of the requested personal data**

“[Name] [Address]

[Date]

Dear [Name of data subject]

**Data Protection subject access request**

Thank you for your letter of *[date]* making a data subject access request for *[subject]*.

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example, the personal data might include personal data is ‘legally privileged’ because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Council staff will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely”



## 6. Data Breach Policy

GDPR defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

The Town Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

### **Consequences of a personal data breach**

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

### **The Town Council's duty to report a breach**

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

If the ICO is not informed within 72 hours, the Town Council must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, the Town Council must:

- i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- ii. Communicate the name and contact details of the key contact
- iii. Describe the likely consequences of the breach
- iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.

When notifying the individual affected by the breach, the Town Council must provide the individual with (ii)-(iv) above.

The Town Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

**Data processors duty to inform the Town Council**

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify the Town Council without undue delay. It is then the Town Council’s responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

**Records of data breaches**

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

**Record of Data Breaches**

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring

To report a data breach use the ICO online system: <https://ico.org.uk/for-organisations/report-a-breach/>

# 7. Document Retention Policy

## Introduction

The Town Council recognises that efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the association. This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Retention Schedule

## Scope

This policy applies to all records created, received or maintained by the Town Council in the course of carrying out its functions.

Records are defined as all those documents which facilitate the business carried out by the Town Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activities.

These records may be created, received or maintained in hard copy or electronically.

A small percentage of the Town Council records may be selected for permanent preservation as part of the Councils archives and for historical research.

## Responsibilities

The Town Council has a corporate responsibility to maintain its records and record management systems in accordance with the regulatory environment.

The person with overall responsibility for this policy is the Town Clerk. The person responsible for records management will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and timely.

Individual staff and employees must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the Town Council's records management guidelines.

### Keynsham Town Council - Appendix A: List of Documents for Retention or Disposal

Document	Minimum Retention Period	Reason	Disposal
Minutes	Indefinite	Archive	Original signed paper copies of Council minutes of meetings must be kept indefinitely in safe storage. At regular intervals of not more than 5 years they must be archived and deposited with the Higher Authority
Agendas	5 years	Management	Bin (shred confidential waste)
Accident/incident reports	20 years	Potential claims	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Scales of fees and charges	6 years	Management	Bin
Receipt and payment accounts	Indefinite	Archive	N/A
Receipt books of all kinds	6 years	VAT	Bin
Bank statements including deposit/savings accounts	Last completed audit year	Audit	Confidential waste
Bank paying-in books	Last completed audit year	Audit	Confidential waste

Document	Minimum Retention Period	Reason	Disposal
Cheque book stubs	Last completed audit year	Audit	Confidential waste
Quotations and tenders	6 years	Limitation Act 1980 (as amended)	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Paid invoices	6 years	VAT	Confidential waste
Paid cheques	6 years	Limitation Act 1980 (as amended)	Confidential waste
VAT records	6 years generally but 20 years for VAT on rents	VAT	Confidential waste
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)	Confidential waste
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal injury (best practice)	Bin
Wages books/payroll	12 years	Superannuation	Confidential waste
Insurance policies	While valid (but see next two items below)	Management	Bin
Insurance company names and policy numbers	Indefinite	Management	N/A
Certificates for insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (SI 2753) Management	Bin

Document	Minimum Retention Period	Reason	Disposal
Town Park equipment inspection reports	21 years		
Investments	Indefinite	Audit, Management	N/A
Title deeds, leases, agreements, contracts	Indefinite	Audit, Management	N/A
Members' allowances register	6 years	Tax, Limitation Act 1980 (as amended)	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Information from other bodies e.g. circulars from county associations, NALC, principal authorities	Retained for as long as it is useful and relevant		Bin
Local/historical information	Indefinite – to be securely kept for benefit of the Parish	Councils may acquire records of local interest and accept gifts or records of general and local interest in order to promote the	N/A
		use for such records (defined as materials in written or other form setting out facts or events or otherwise recording information).	
Magazines and journals	Council may wish to keep its own publications	The Legal Deposit Libraries Act 2003 (the	Bin if applicable

GDPR Policies and Procedures  
First Adopted, 21<sup>st</sup> January 2025 – Review Date 22d January 2027

Document	Minimum Retention Period	Reason	Disposal
	For others retain for as long as they are useful and relevant.	2003 Act) requires a local council which after 1 <sup>st</sup> February 2004 has published works in print (this includes a pamphlet, magazine or newspaper, a map, plan, chart or table) to deliver, at its own expense, a copy of them to the British Library Board (which manages and controls the British Library). Printed works as defined by the 2003 Act published by a local council therefore constitute materials which the British Library holds.	
<b>Record-keeping</b>			
To ensure records are easily accessible it is necessary to comply with the following: <ul style="list-style-type: none"> <li>• A list of files stored in cabinets will be kept</li> <li>• Electronic files will be saved using relevant file names</li> </ul>	The electronic files will be backed up periodically on a portable hard drive and also in the cloud-based programme supplied by the Council's IT company.	Management	Documentation no longer required will be disposed of, ensuring any confidential documents are destroyed as confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.

Document	Minimum Retention Period	Reason	Disposal
<b>General correspondence</b>	Unless it relates to specific categories outlined in the policy, correspondence, both paper and electronic, should be kept. Records should be kept for as long as they are needed for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests.	Management	<b>Bin (shred confidential waste)</b> <b>A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.</b>
<b>Correspondence relating to staff</b>	If related to Audit, see relevant sections above. Should be kept securely and personal data in relation to staff should not be kept for longer than is necessary for the purpose it was held. Likely time limits for tribunal claims between 3–6 months Recommend this period be for 3 years	After an employment relationship has ended, a council may need to retain and access staff records for former staff for the purpose of giving references, payment of tax, national insurance contributions and pensions, and in respect of any related legal claims made against the council.	<b>Confidential waste</b> <b>A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.</b>
<b>Documents from legal matters, negligence and other torts</b> Most legal proceedings are governed by the Limitation Act 1980 (as amended). The 1980 Act provides that legal claims may not be commenced after a specified period. Where the limitation periods are longer than other periods specified the			



Document	Minimum Retention Period	Reason	Disposal
documentation should be kept for the longer period specified. Some types of legal proceedings may fall within two or more categories.			
Document	Minimum Retention Period	Reason	Disposal
If in doubt, keep for the longest of the three limitation periods.			
Negligence	6 years		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Defamation	1 year		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Contract	6 years		Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Leases	12 years		Confidential waste.
Sums recoverable by statute	6 years		Confidential waste.
Personal injury	3 years		Confidential waste.
To recover land	12 years		Confidential waste.
Rent	6 years		Confidential waste.
Breach of trust	None		Confidential waste.

Document	Minimum Retention Period	Reason	Disposal
<b>Trust deeds</b>	Indefinite		N/A
<b>For Halls, Centres, Recreation Grounds</b>			
<ul style="list-style-type: none"> <li>• Application to hire</li> <li>• Invoices</li> <li>• Record of tickets issued</li> </ul>	6 years	VAT	Confidential waste A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
<b>Lettings diaries</b>	Electronic files linked to accounts	VAT	N/A
<b>Terms and Conditions</b>	6 years	Management	Bin
Document	Minimum Retention Period	Reason	Disposal
<b>Event Monitoring Forms</b>	6 years unless required for claims, insurance or legal purposes	Management	Bin. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
<b>For Allotments</b>			
<b>Register and plans</b>	Indefinite	Audit, Management	N/A
<b>Minutes</b>	Indefinite	Audit, Management	N/A
<b>Legal papers</b>	Indefinite	Audit, Management	N/A
<b>For Burial Grounds</b>			

Document	Minimum Retention Period	Reason	Disposal
<ul style="list-style-type: none"> <li>• Register of fees collected</li> <li>• Register of burials</li> <li>• Register of purchased graves</li> <li>• Register/plan of grave spaces</li> <li>• Register of memorials</li> <li>• Applications for interment</li> <li>• Applications for right to erect memorials</li> <li>• Disposal certificates</li> <li>• Copy certificates of grant of exclusive right of burial</li> </ul>	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI 204)	N/A
<b>Planning Papers</b>			
Applications	1 year	Management	Bin
Appeals	1 year unless significant development	Management	Bin
Trees	1 year	Management	Bin
Local Development Plans	Retained as long as in force	Reference	Bin
Local Plans	Retained as long as in force	Reference	Bin
Town/Neighbourhood Plans	Indefinite – final adopted plans	Historical purposes	N/A
<b>CCTV</b>			
Daily notes	Daily	Data protection	Confidential waste
Radio rotas	1 week	Management	Confidential waste

Document	Minimum Retention Period	Reason	Disposal
Work rotas	1 month	Management	Confidential waste
Observation sheets	3 years	Data protection	Confidential waste
Document	Minimum Retention Period	Reason	Disposal
Stats	3 years	Data protection	Confidential waste
Signing in sheets	3 years	Management	Confidential waste
Review requests	3 years	Data protection	Confidential waste
Discs – master and working	For as long as required	Data protection	Confidential waste
Internal Operations Procedure Manual	Destroy on renewal Review annually	Management	Confidential waste
Code of Practice	Destroy on renewal Review annually	Management	Confidential waste
Photographs/digital prints	31 days	Data protection	Confidential waste

## 8. Template Data Consent Form

Your privacy is important to us and we would like to communicate with you about the council and its activities. To do so we need your consent. Please fill in your name and address and other contact information below and confirm your consent by ticking the boxes below.

		<i>If you are aged 13 or under your parent or guardian should fill in their details below to confirm their consent</i>
<b>Name</b>		
<b>Address</b>		
<b>Signature</b>		
<b>Date</b>		

Please confirm your consent below. You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the Council Offices (see header).

You can withdraw or change your consent at any time by contacting the council office.

- We may contact you** to keep you informed about what is going on in the Council's area or other local authority areas including news, events, meetings, clubs, groups and activities. These communications may also sometimes appear on our website, or in printed or electronic form (including social media).
- We may contact you** about groups and activities you may be interested in.
- We may use** your name and photo in our newsletters, bulletins or on our website, or our social media accounts (for example Facebook or Twitter).

### Keeping in touch:

- Yes please**, I would like to receive communications by email.
- Yes please**, I would like to receive communications by telephone.
- Yes please**, I would like to receive communications by mobile phone (including texts).
- Yes please**, I would like to receive communications by social media.
- Yes please**, I would like to receive communications by post.





