Data Protection Policy

INDEX OF LYDBROOK PARISH COUNCIL DATA PROTECTION POLICY

1 About this Policy

1.1 This policy outlines the standards Lydbrook Parish Council ('the Council') intends to observe in relation to its compliance with the General Data Protection Regulation (GDPR) and subsequently revised UK Data Protection law.

1.2 The policy is applicable to all councillors and any employees, partners, voluntary groups, third parties and agents authorised by them.

1.3 The Council shall ensure that all users fully understand its obligations and have undertaken the necessary training to demonstrate compliance with this policy.

1.4 This policy applies to all personal information created or held by the Council, in whatever format. This includes, but is not limited to paper, electronic, mail, microfiche and film.

2 Responsibilities

2.1 To operate efficiently, the Council must collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, customers, contractors, suppliers and partner organisations.

2.2 The Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business. The Council will, therefore, ensure that it treats personal information correctly in accordance with the law.

2.3 The Council as a whole is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to the clerk, who will undertake information audits and manage the information collected by the Council including the issuing of privacy notices, dealing with requests and complaints raised and the safe disposal of information.

2.4 Councillors who process personal data on an individual basis and are not acting on behalf of the council are likely to be considered data controllers and therefore required to notify the Information Commissioner's Office.

2.5 All councillors and officers who hold or collect personal data are responsible for compliance with data protection legislation and must ensure that personal and/or sensitive information is kept and processed in accordance with this policy:

3 Legal Framework

3.1 Breach of this policy may result in disciplinary action in accordance with the Council's Conduct and, in certain circumstances may be considered to be gross misconduct, resulting in dismissal. It should also be noted that breach of the policy could also lead to criminal or civil action if illegal material is involved or legislation is contravened. Councillors found to be in breach of this policy may also be deemed to have breached the Code of Conduct and referred to the District Council's Monitoring Officer.

4 Privacy by Design

4.1 The GDPR requires data controllers to put measures in place to minimise personal data processing and that they only process data that is necessary for the purposes of processing and stored for as long as is necessary.

4.2 The Council will have the appropriate measures in place to determine the basis for lawful processing and will undertake risk assessments to ensure compliance with the law. These measures include the use of Data Protection Impact Assessments (DPIAs).

5 Contracts

5.1 Data protection law places requirements on both the Council and its suppliers to ensure the security of personal data, and to manage individuals' privacy rights. This means that whenever the Council uses a supplier to process individuals' data on its behalf it must have a written contract in place.

5.2 The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

5.3 The Council is liable for its compliance with data protection law and must only appoint suppliers who can provide 'sufficient guarantees' that the requirements of the law will be met, and the rights of individuals protected.

5.4 If a contractor, partner organisation or agent of the Council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, or if they will do so as part of the services they provide to the Council, the relevant lead Councillor or Council officer must ensure that personal data is managed in accordance with data protection law and this Policy.

5.5 Security and data protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council and reviewed during the contract's life cycle.

5.6 Council officers will use the appropriate processes, templates and DPIAs when managing or issuing contracts.

6 Information Sharing

6.1 The Council may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

6.2 Information must always be shared in a secure and appropriate manner and in accordance with the information type. The Council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

6.3 Any Councillor or officer dealing with telephone enquiries must be careful about disclosing personal information held by the Council. In order to manage this the enquirer will be asked to put their request in writing in the first instance.

7 Individuals' Rights

7.1 An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR). Information on how an individual can make a SAR can be found at Appendix 2.

7.2 Individuals also have other rights under the Data Protection Act 2018 which are set out in the Council's privacy notices (see Appendix 1). The Council must respond to individuals exercising their rights within one month.

8 Disclosure of Personal Information to Third Parties

8.1 Personal data can only be disclosed about a third party in accordance with the Data Protection Act 2018.

8.2 If a user believes it is necessary to disclose information about a third party to a person requesting data, they must seek specialist advice before doing so.

9 Breach of Information Security

9.1 The Council understands the importance of recognising and managing information security incidents. This occurs when data or information is transferred to somebody who is not entitled to receive it. It includes losing data or theft of information, unauthorised use of the Council's system to process or store data by any person or attempted unauthorised access to data or information regardless of whether this was successful or not.

9.2 All users have an obligation to report actual or potential data protection compliance failures as soon as possible and take immediate steps to minimise the impact and to assist with managing risk. The Council will fully investigate (see Appendix 3) both actual and potential failures and take remedial steps, if necessary, maintain a register of compliance failures. If the incident involves or impacts personal data, it must be reported to the ICO within 72 hours.

10 IT and Communications Systems

10.1 This section and sections 11, 12, 13, 14, 15 and 16 must be read in conjunction with Lydbrook Parish Council's IT policy.

10.2 The Council's IT and communications systems are intended to promote effective communication and working practices. This policy outlines the standards users must observe when using these systems and the action the Council will take if users breach these standards.

10.3 Breach of this policy may be dealt with under the Council's Disciplinary Procedure and, in serious cases, may be treated as gross misconduct.

11 Equipment Security and Passwords

11.1 Councillors and officers are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy. Passwords must be set on all IT equipment and passwords must remain confidential and be changed regularly.

11.2 Users must only log onto Council systems using their own username and password. Users must not use another person's username and password or allow anyone else to log on using their username and password.

12 Systems and Data Security

12.1 Users should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

12.2 Users must not download or install software from external sources. Downloading unauthorised software may interfere with the Council's systems and may introduce viruses or other malware.

12.3 Users must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems.

12.4 Users should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

12.5 Users must inform the clerk immediately if they suspect a computer may have a virus.

13 E-Mail

13.1 Users should adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail.

13.2 It should be noted that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

13.3 Users must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

13.4 For the purposes of council business, users must use a designated email account (or only use the email account provided) in order to receive or send email correspondence.

14 Using the Internet

14.1 Users should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

15 Prohibited use of Council Systems

15.1 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under the Council's Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

15.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or our local community;

(c) a false and defamatory statement about any person or organisation;

(d) material, which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

(e) confidential information about the Council or any of our staff or our community (except as authorised in the proper performance of your duties);

(f) unauthorised software;

(g) any other statement which is likely to create any criminal or civil liability; or

(h) music or video files or other material in breach of copyright.

16 Bring Your Own Device (BYOD)

16.1 The Council must take appropriate technical and organisational measures against accidental loss or destruction of or damage to personal data. Councillors using their own devices raises a number of data protection concerns due to the fact that these are owned by the user rather than the data controller. The risks the controller needs to assess are:

- The type of data held.
- Where the data may be stored.
- How the data is transferred.
- Potential data leakage.
- Blurring of personal and business use.
- The device's security capacities.
- What to do if the person who owns the device leaves the Council and
- How to deal with the loss, theft, failure and support of a device.

Councillors and officers using their own devices shall have the following responsibilities:

- Users will not lend their device to anybody.
- Users will inform the Council should they lose, sell, recycle or change their device.
- Users will enable a security pin to access their device and an automatic lock every 5 minutes requiring re-entry of the pin.
- Users will ensure security software is set up on their device and kept up to date.
- Users will not use their device to store Council emails, files and data.

17 Social Media

17.1 This policy is in place to minimise the risks to our Council through use of social media and must be read in conjunction with Lydbrook Parish Council's Media and Social Media policy.

17.2 This policy deals with the use of all forms of social media, including Facebook and all other social networking sites, internet postings and blogs. It applies to use of social media for Council purposes as well as personal use that may affect our business in any way.

17.3 Users must avoid making any social media communications that could damage the Council's interests or reputation, even indirectly.

17.4 Users must not use social media to defame or disparage us, Council staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

17.5 Any misuse of social media should be reported to the clerk.

17.6 Users should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf.

17.7 Be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.

17.8 A data protection breach may result in disciplinary action up to and including dismissal.

17.9 Members or staff may be required to remove any social media content that the Council believes constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

18 Records Management & Retention

Records will be maintained in line with the **Local Government Association retention schedule**.

The Retention Schedule, below, sets out how long the parish council will keep different categories of records before they are securely disposed of or archived. It supports compliance with the UK GDPR, the Data Protection Act 2018, and relevant statutory requirements.

The schedule applies to all formats, including paper, electronic files, emails, photographs, audio, and video.

- **Governance & Administration**

Record Type	Retention Period	Notes
Signed Council Minutes	Permanent	Archive as historical record
Draft Minutes	Until approved	Destroy after approval
Agendas	5 years	Good practice
Councillor Declarations of Acceptance of Office	Term of office + 1 year	Governance requirement
Register of Members' Interests	As long as current + 1 year	Legal requirement
Policies & Procedures	Current version + 1 year	Keep superseded versions for audit trail

- **Finance & Audit**

Record Type	Retention Period	Notes
Annual Accounts	7 years	Audit & HMRC
Bank Statements	7 years	HMRC
VAT Records	6 years (except Rents - 20 years)	VAT
Invoices & Receipts	7 years	HMRC
Investments	Permanent	Audit, Management
Audit Reports	7 years	Good practice
Grants Awarded	6 years	Audit
Grants Received	6 years	Audit

- **Human Resources**

Record Type	Retention Period	Notes
Employee Personnel Files	6 years after employment ends	Limitation Act
Timesheets	Last completed audit year 3 years	Audit Personal Injury (Best practice)

Payroll Records	6 years	HMRC
Pension Records	6 years	HMRC
Recruitment Records (unsuccessful applicants)	6 months	Good practice
Training Records	3 years	Administrative

- **Contracts & Legal**

Record Type	**Retention Period**	**Notes**
Quotations and Tenders	6 years	Limitation Act
Contracts (suppliers, services)	6 years after expiry	Limitation Act
Leases & Property Agreements	Duration of lease + 6 years	Legal requirement
Insurance Policies	6 years	Limitation Act
Insurance Claims	6 years	Limitation Act
Certificates for Insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability

- **Health & Safety**

Record Type	**Retention Period**	**Notes**
Accident/Incident Reports (adults)	3 years	H&S
Accident/Incident Reports (children)	25 years	H&S
Risk Assessments	Until superseded + 3 years	Good practice

- **Assets & Property**

Record Type	**Retention Period**	**Notes**
Title Deeds, Leases, Agreements, Contracts	Permanent	Audit, Management
Asset Register	Permanent	Historical record
Maintenance Records	6 years	Limitation Act
Cemetery/Burial Records (if applicable)	Permanent	Historical & Legal

- **Planning**

Record Type	Retention Period	Notes
Planning Applications (copies)	1 year	Principal authority holds originals
Planning Responses	3 years	Administrative

- **Communications & Media**

Record Type	Retention Period	Notes
Newsletters	2 years	Administrative
Website Content	Until superseded	Administrative
Social Media Posts	1 year	Administrative

When records reach the end of their retention period, they must be destroyed securely:

- Paper: cross-cut shredding or confidential waste service
- Electronic: permanent deletion from all devices and backups
- Special category data: additional care and disposal logging.

19 Policy Review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

Appendix 1 – Privacy Notice (Staff/Volunteers)

1. WHAT INFORMATION WE COLLECT AND USE, AND WHY

Staff recruitment, administration and management

We collect or use the following personal information as part of **staff recruitment, administration and management**:

- Contact details (e.g. name, address, telephone number or personal email address)
- Next of kin or emergency contact details

Salaries and pensions

We collect or use the following personal information as part of **managing salaries and pensions**:

- Job role and employment contract (e.g. start and leave dates, salary, changes to employment contract or working patterns)
- Time spent working (e.g. timesheets or clocking in and out)
- Expense, overtime or other payments claimed
- Leave (e.g. sick leave, holidays or special leave)
- Maternity, paternity, shared parental and adoption leave and pay
- Pension details
- Bank account details
- Payroll records
- Tax status

2. LAWFUL BASES AND DATA PROTECTION RIGHTS

Under UK data protection law, we must have a "lawful basis" for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO's website.

Which lawful basis we rely on may affect your data protection rights which are set out in brief below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:

- **Your right of access** - You have the right to ask us for copies of your personal information. You can request other information such as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. Read more about the right of access.
- **Your right to rectification** - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. Read more about the right to rectification.

- **Your right to erasure** - You have the right to ask us to delete your personal information. Read more about the right to erasure.
- **Your right to restriction of processing** - You have the right to ask us to limit how we can use your personal information. Read more about the right to restriction of processing.
- **Your right to object to processing** - You have the right to object to the processing of your personal data. Read more about the right to object to processing.
- **Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. Read more about the right to data portability.
- **Your right to withdraw consent** – When we use consent as our lawful basis you have the right to withdraw your consent at any time. Read more about the right to withdraw consent.

If you make a request, we must respond to you without undue delay and in any event within one month.

To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

3. OUR LAWFUL BASES FOR THE COLLECTION AND USE OF YOUR DATA

Our lawful bases for collecting or using personal information as part of **staff recruitment, administration and management** are:

- Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Our lawful bases for collecting or using personal information as part of **managing salaries and pensions** are:

- Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

4. WHERE WE GET PERSONAL INFORMATION FROM

We collect your information from the following places:

- Directly from you

5. HOW LONG WE KEEP INFORMATION

For more information about how long we keep your information refer to Section 8 – Records Management & Retention of this Policy document.

6. WHO WE SHARE INFORMATION WITH

In some circumstances, we may share information with the following organisations:

- HMRC

- Data processors

  We use the following data processors for the following reasons:

  Kingscott Dix accountants

  This data processor does the following activities for us: Process payroll

7. HOW TO COMPLAIN

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

Website: https://www.ico.org.uk/make-a-complaint

Appendix 2 – Subject Access Request (SAR) Procedure

1. Purpose of this Procedure

This procedure sets out how the Parish Council will handle Subject Access Requests (SARs) made by individuals wishing to access personal data held about them. It ensures compliance with UK GDPR and promotes transparency and accountability.

2. What is a Subject Access Request?

A SAR is a request made by an individual (the "data subject") asking for:

- Confirmation that the Council processes their personal data
- Access to that personal data
- Supplementary information required under UK GDPR

A SAR can be made **in writing or electronically**, including by email or social media.

3. Receiving a SAR

- Any councillor or employee who receives a SAR **must forward it immediately to the Clerk**, who is the Council's Data Protection Lead.
- The request will be logged using the SAR Log Form (see below); initially recording the following information:
    - Date received
    - Name and contact details of requester
    - Summary of the request
    - Deadline for response (one month from receipt)

4. Verifying Identity

Before responding, the Council must take reasonable steps to verify the requester's identity. Acceptable evidence may include:

- Passport or driving licence
- Utility bill or bank statement (recent)

The one-month response period begins **once identity is confirmed**.

5. Clarifying the Request (if needed)

If the request is broad or unclear, the Council may ask the requester to clarify:

- Specific time periods
- Specific services or interactions
- Specific documents or correspondence

The response deadline is paused until clarification is received.

6. Searching for Information

All councillors and staff must conduct a **full and exhaustive search** of records they hold that may contain personal data relating to the requester.
This includes:

- Emails
- Paper files
- Minutes (including draft or handwritten notes)
- Spreadsheets, databases, or logs
- CCTV (if applicable)
- Correspondence with contractors or third parties

Searches must be proportionate but thorough.

7. Applying Exemptions

Some information may be withheld if an exemption applies, such as:

- Personal data about another individual
- Legally privileged information
- Data relating to crime or taxation
- Confidential references

Where data is withheld, the Council must explain why (unless doing so would itself breach an exemption).

8. Preparing the Response

The Council must provide:

- A copy of the requester's personal data
- The purposes for which it is processed
- Categories of data
- Recipients or categories of recipients
- Retention periods
- Information about rights to rectification, erasure, restriction, and complaint
- Source of the data (if not collected directly)

Data should be supplied in a **commonly used electronic format** unless the requester asks otherwise.

9. Response Timescale

- The Council must respond **within one month** of receiving the request.

- This may be extended by **up to two further months** if the request is complex or numerous.
- The requester must be informed of any extension within the first month.

10. Fees

SARs must be provided **free of charge**.
A reasonable fee may be charged only if the request is:

- Manifestly unfounded
- Excessive
- Repetitive

11. Record Keeping

The Clerk must maintain a SAR log including:

- Date received
- Identity verification date
- Searches conducted
- Data supplied
- Exemptions applied
- Date of response
- Any fees charged

This supports accountability and audit compliance.

12. Right to Complain

The response must inform the requester that they may complain to:

- The Parish Council (initially)
- The Information Commissioner's Office (ICO)

Subject Access Request (SAR) Log Form

1. Request Details

- **Reference Number:** _____
- **Date Received:** _____
- **Method Received (email/letter/in person/other):** _____

2. Requester Information

- **Full Name:** _____
- **Address:** _____
- **Email:** _____
- **Telephone:** _____

3. Identity Verification

- **Identity Verified? (Y/N):** _____
- **Verification Method (passport, driving licence, utility bill, etc.):** _____
- **Date Verified:** _____

4. Summary of Request

Describe the personal data the requester is seeking:

_____

_____

_____

5. Clarification (if required)

- **Was clarification requested? (Y/N):** _____
- **Date clarification requested:** _____
- **Date clarification received:** _____

6. Searches Conducted

Systems/locations searched (tick or list):

- Clerk's email
- Councillors' emails
- Paper files
- Minutes/agendas
- CCTV
- Third-party processors

- Other (specify): _____

Details of searches:

---

7. Exemptions Applied

- **Were any exemptions applied? (Y/N): _____**
- **Details of exemptions (e.g., third-party data, legal privilege):**

---

8. Response

- **Date response sent: _____**
- **Was an extension applied? (Y/N): _____**
- **If yes, reason for extension:**

- **Was a fee charged? (Y/N): _____**
- **If yes, reason for fee:**

---

9. Notes / Follow-up

Appendix 3 – Data Breach Procedure

1. Purpose of this Procedure

This procedure sets out how the Parish Council will identify, manage, and report personal data breaches in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Its purpose is to ensure prompt action, minimise harm, and maintain public trust.

2. Definition of a Data Breach

A personal data breach is any incident that results in:

- Unauthorised access to personal data
- Unauthorised disclosure of personal data
- Loss of personal data
- Destruction or alteration of personal data
- Loss of availability of personal data

Examples include:

- Sending personal data to the wrong recipient
- Loss or theft of a laptop, USB stick, or paper file
- Email accounts being compromised
- Accidental deletion of important personal data
- Unauthorised access by councillors, staff, or third parties

3. Responsibilities

- The Clerk is the Council's Data Protection Lead and is responsible for coordinating breach investigations and reporting.
- All councillors, employees, and volunteers must report suspected breaches immediately.
- The Council is responsible for ensuring appropriate technical and organisational measures are in place to prevent breaches.

4. Identifying a Breach

Any person who becomes aware of a potential data breach must report it immediately to the Clerk, providing:

- A description of the incident
- The type of personal data involved
- Who is affected
- When and how the breach was discovered

Delays in reporting may increase harm and risk non-compliance.

5. Initial Assessment

Upon receiving a report, the Clerk will:

1. Record the incident in the Data Breach Log
2. Assess whether personal data is involved
3. Determine the potential impact on individuals
4. Decide whether urgent containment action is required

If the Clerk is unavailable, the Chair of the Council will assume responsibility.

6. Containment and Recovery

The Clerk will take immediate steps to limit the breach, which may include:

- Stopping unauthorised access
- Recovering lost data
- Resetting passwords
- Suspending affected systems
- Contacting third party processors

All actions must be recorded.

7. Risk Assessment

The Clerk will assess the likelihood and severity of the risk to individuals' rights and freedoms, considering:

- The type and sensitivity of the data
- The volume of data involved
- Whether individuals can be identified
- Potential consequences (e.g., identity theft, distress, financial loss)
- Whether vulnerable individuals are affected

8. Reporting to the ICO

If the breach is likely to result in a risk to individuals, the Council must report it to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.

The report must include:

- Nature of the breach
- Categories and approximate number of individuals affected
- Categories and approximate number of data records involved
- Likely consequences
- Measures taken or proposed to address the breach

If the Council decides not to report the breach, the reasoning must be documented.

9. Notifying Individuals

If the breach is likely to result in a high risk to individuals, the Council must notify affected individuals without undue delay, explaining:

- What happened
- What data was involved
- Potential consequences
- What the Council is doing to address the breach
- What individuals can do to protect themselves
- Contact details for further information

10. Documentation

All breaches, whether reportable or not, must be recorded in the Data Breach Log, including:

- Date and time discovered
- Description of the breach
- Actions taken
- Decisions made
- Whether the ICO or individuals were notified
- Lessons learned

11. Prevention Measures

The Council will take reasonable steps to prevent future breaches, including:

- Regular password updates
- Secure storage of paper and electronic records
- Staff and councillor training
- Reviewing data retention practices
- Ensuring third party processors meet GDPR standards