ALL SAINTS
PARISH COUNCIL
Creating a Parish where the community feels as one

All Saints Parish Council

Data Protection Roadmap

NALC Data Protection – Assertion 10 AGAR Guidance

Document History	Revision Date	Minute
Based on NALC Data Protect Roadmap – November 2025	This version 1.0 – REVIEWED February 2026 and ADOPTED at the Council meeting held on 3 March 2026	Minute (OM26/098 I)

ALL SAINTS PARISH COUNCIL
Creating a Parish where the community feels as one

Table of Contents

1 Introduction

1.1 Building confidence in data protection

Data protection may feel daunting for parish and town councils. The rules are complex, the language is often technical, and clerks and councillors already wear many hats, meaning it can sometimes slip down the list of priorities. Yet data protection is a core part of council governance, essential for protecting people's rights and maintaining public trust. This data protection roadmap has been designed to make the task easier. It provides a confidence-building starting point, written in plain English, to help councils of all sizes understand their responsibilities, take practical steps, and feel more in control of data protection matters.

From 2025/26, the Annual Governance and Accountability Return (AGAR) will require smaller authorities to confirm they have appropriate data protection measures in place. While this does not create new obligations, it does bring existing responsibilities into sharper focus, emphasising the importance of proactive data protection practices. The new Assertion 10 goes beyond legal compliance; it's an opportunity to build public trust and demonstrate professionalism in serving your community.

1.2 Why this roadmap?

This roadmap breaks down data protection into four clear stages:

1. Mapping what data you hold and why
2. Identifying the lawful basis for each purpose
3. Assessing risks and protecting people's rights

4. Creating policies and embedding good practice

Each stage provides plain English explanations of key concepts, supported by checklists, reflective questions, and worked examples to help you apply the steps in your own council.

Where more detail is needed, we signpost you to authoritative resources from the Information Commissioner's Office (ICO), so you can explore further with confidence.

1.3 Key principles to keep in mind

At its heart, data protection is about respecting people's right to privacy. It ensures that individuals' personal data is handled with care, fairness, and transparency. The law is based on seven key principles, which guide everything you do with personal data.

Achieving compliance should be seen as a journey, and not a one-off task. The journey is most effective when each stage is approached methodically, rather than trying to complete everything at once. By working through the stages in order, your council will build a strong foundation and sustainable framework.

It is also important to remember that every council is unique. This roadmap is designed to help you make decisions that fit your council's size, functions, and resources, rather than follow a one-size-fits-all template.

Finally, good data protection builds trust. It reassures residents and stakeholders that their information is safe, reduces the risk of complaints, and gives councillors and staff confidence that they are acting responsibly.

1.4 How to use this roadmap

Work through each stage in order, and resist the urge to jump to the final stage. Refer to the checklists and questions to guide your thinking. Use the examples to spark ideas, and adapt them to your council's circumstances. Record your decisions as you go - your documentation will become the central reference point for all your data protection work.

By the end, your council will have:

- A clear picture of what personal data you process and why.
- Considered data protection principles, and documented lawful bases and risk decisions.
- Policies and a notice that explains your approach.
- Embedded practices that make compliance part of everyday council business.

This roadmap is not about perfection or legal jargon. It is about giving parish and town councils the confidence, structure, and tools to make data protection manageable and meaningful.

1.5 Author

We've partnered with **Breakthrough Communications** as our specialist provider for data protection and information compliance support. Breakthrough Communications works extensively with parish and town councils, delivering expert training, tailored guidance, and practical resources that help councils meet their data protection responsibilities with confidence. Their approach is clear, practical, and achievable, designed to reduce risk, safeguard personal data, and support councils in operating transparently while maintaining public trust.

2 Stage One

2.1 Goal of Mapping Your Data

Work out what personal data your council processes and why.

2.1.1 What counts as personal data?

Personal data is any information that can identify a living person, either directly (e.g. name) or indirectly (e.g. email, job title, address, reference number). It applies to records in any format, including digital files, paper documents, audio and video.

A simple test: Ask yourself, can this information identify who the person is, either on its own or when it's combined with other details?

- If yes, it is personal data.

- If no, it is not personal data.

You should not consider how likely it is; the test is whether identification is possible at all, yes or no.

2.2 Why map your personal data?

Mapping shows what personal data your council processes, why you have it, and how it is managed and used. Every council is unique (e.g. functions, scale, resources), so no other council's approach will fit your council. Data mapping helps you to identify and clarify all the purposes for which your council processes personal data, which can be many and varied, even between councils.

All councils collect or use personal data in some way, even if it isn't immediately obvious. This means every council must comply with data protection law and be **registered** with the Information Commissioner's Office (ICO). Your council is a data controller, which means it is legally responsible for making sure personal data is handled properly and in line with the law.

Data mapping is a simple process of identifying and recording the personal data your council processes. It is the first step in building a strong and practical data protection framework.

2.3 Data mapping in practice

A data map can be a simple table that records every purpose your council has for processing personal data. It shows the types of personal data involved, whether the data is shared with other organisations or handled by data processors on the council's behalf. It will also record the lawful basis which allows the council to process the data and identify if any special category data is being processed (more in Stage Two).

Here is an example Data Map:

Purpose of processing	Categories of personal data	Categories of recipients (sharing)*	Categories of Processors (data processors on behalf of data controller)	Names of third countries or international organisations that personal data are transferred to (if applicable)	Retention schedule **
Minutes	Identity, Contact information	N/A	Cloud storage provider, Website provider	European Union	Indefinite
Accounts	Identity, Contact information, Bank Details	HMRC	Accounts software provider, Cloud storage provider,	European Union	X years after current year
Correspondence and Casework	Identity, Contact Information, Special category data	Other Local Authority, Law enforcement and similar competent authorities	Cloud storage provider,	European Union	X years after completion of matter
Payroll and Pensions	Identity, Contact information, Bank Details	HMRC, pension provider	Accounts software provider, Cloud storage provider,	European Union	X years after current year
HR files	Identity, Contact information, Special Category Data	N/A	Cloud storage provider, HR consultants	European Union	X years after employment ends

* "Recipients (sharing)" means other data controllers you share data with.
** Data protection law does not specify data retention periods. Councils will need to consider their own needs, as well as other laws, regulations, and best practices, for each purpose identified.

Heading explanations:

- Purpose of processing — Why are you using the data? e.g. taking minutes, managing payroll.
- Categories of personal data — What types of personal information are involved? For example, contact information, bank details.
- Categories of recipients (sharing) — Who do you share the data with, outside the council? For example, other data controllers such as HMRC.
- Categories of processors — Any companies or people who process data for the council, but don't decide how it's used. For example, a website host, an email provider, and a cloud software provider.
- Names of third countries or international organisations that personal data is transferred to — Identify whether data is processed outside the UK, and if so, where.
- Retention schedule — How long you keep data before deleting or archiving it.

2.4 Checklist

- Identify all council functions and services (broad areas: meetings, services, facilities, finance). This will give you a basic structure to begin your data map.
- For each function or service, list your purpose(s) for processing personal data (e.g. producing minutes, administering allotments, etc).
- For each purpose, complete a row in the data map (**use the ICO template**).
- Identify any data controllers for each purpose (i.e. organisations or persons the council shares data with), such as HMRC, banks, or other local authorities.
- Identify any data processors for each purpose (i.e. suppliers that process the council's data on their behalf), such as website hosts, cloud storage providers, email services, payroll providers, etc.
- Identify where any data leaves the UK (international transfers), which is common with cloud-based systems, and will require additional safeguards (see Stage Three).

2.5 Top tips

Take your time with this task. Careful thought and clear documentation save time and avoid risks later. The more thorough and detailed your map, the easier the next stages will be.

- Save your data map on a secure network, labelled clearly for future reference. It will form the basis of your data protection compliance.
- Set a review date for each purpose to ensure the map stays up to date.
- Share your draft map with other team members to ensure its accuracy.
- Don't forget to check legacy records such as paper files and archived records.

2.6 Time to reflect

Consider the following questions as part of your data mapping process, giving regard to the data protection principles of data minimisation and storage limitation:

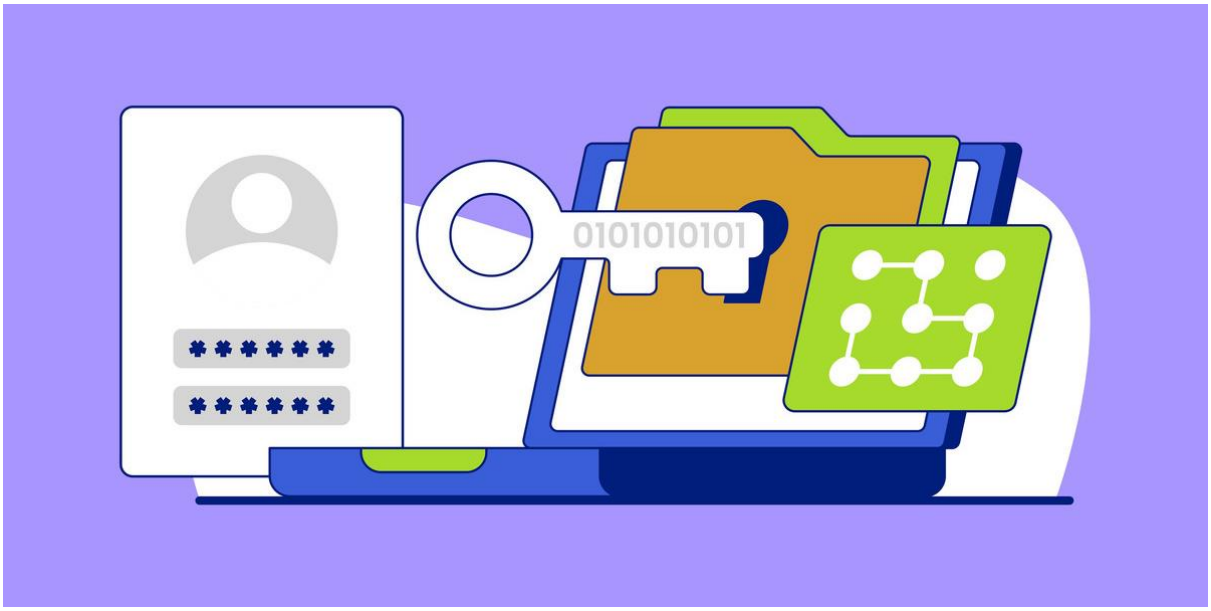
- Could we explain to any resident, in plain English, why we hold this data?
- Are we only collecting the information we genuinely need for our purpose?
- Do we hold more personal data than necessary?

- Is the data stored securely?
- Have we decided how long to keep it, and when it's no longer needed?

2.7 Summary of outputs from Stage One

- Created a data map showing how personal data is processed across all council functions and purposes.
- Recognised when the council shares data with other data controllers.
- Identified data processors handling council data on the council's behalf.
- Recorded any international transfers.
- Defined retention periods for each purpose.

3 Stage Two



3.1 Goal of Lawful bases

Identify and record the lawful basis for each purpose in your data map.

3.2 Why this matters

The **UK General Data Protection Regulations** (UK GDPR) require every council to identify a lawful basis for each purpose for processing personal data. This is not optional, even if the matter feels routine. By identifying and recording the lawful basis for each purpose identified in the data map, councils can meet their legal obligations and show evidence that personal data is being processed responsibly.

There are six lawful bases in data protection law. Most of the time, the right basis will be clear, but sometimes you'll have a choice, and it's up to the council to decide the best fit. It's important to think this through carefully and be able to explain your choice, as the lawful basis should be a good match for the way the data is used.

3.3 The six lawful bases

There are six lawful bases that you can use to process personal data, and each one has its own set of requirements (**UK GDPR Article 6(1)**). These bases help you to comply with the data protection principles.

1. Consent — When an individual makes a fully informed decision to agree to processing freely and takes a positive action to demonstrate that consent. Example: a resident signing up for a council newsletter.

2. Contract — When data is needed to deliver a contract that the council has entered into, or when someone wants to have a contract with you. Example: an allotment tenancy.

3. Legal obligation — Where the law requires you to process data. Example: a councillor's register of interest.

4. Vital interests — When processing is necessary to protect someone's life. Example: sharing health information with medical professionals if the person is unable to make decisions for themselves. Note: Rare for councils to use.

5. Public task — Where processing is necessary for a task carried out in the public interest, or in the exercise of official authority given to the council, but there is no legal requirement to do it. Example: answering general correspondence.

6. Legitimate interests — Can be used when no other lawful bases apply, but it requires an additional risk assessment. The assessment is a three-part test, and the ICO provides a **downloadable template** to help with this. Example: CCTV in council buildings. Note: You should only rely on this basis if your processing passes the three-part test.

If the council cannot identify a lawful basis for processing personal data, it must not process that data.

3.4 Special Category Data

Some personal data needs additional safeguards. This is called special category data. It includes personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health, sex life and sexual orientation.

At first glance, you might think your council never touches this kind of data, but it can hide in plain sight and crop up in everyday tasks. So it's important to check carefully when building your data map.

Examples of how special category data can show up:

• A resident includes details about their disability in a request for an accessible allotment plot.
• A staff file records health information, or trade union membership.
• A councillor lists their role on a church council in their Register of Interests, which indirectly reveals their religious belief.

When special category data is identified for a purpose, you must have an extra safeguard in place to allow that processing. This safeguard is called an additional condition to process.

Data protection law requires that special category data be processed only if you have both a normal lawful basis and an additional condition. Some of these additional conditions also require an Appropriate Policy Document (APD) to explain how the data is protected.

An APD is a short document that shows how your council will look after special category data. It explains the steps you take to follow the data protection principles, and sets out your rules on retention and erasure. It doesn't need to be long or complex, just a clear written record that can be shown to the ICO if needed. The ICO provides a simple **downloadable template** to guide you through the questions to cover.

The table below shows the additional conditions to process under **UK GDPR Article 9(2)** and which ones require an APD.

Additional conditions to process (Article 9(2))	**APD required**
(a) Explicit consent	No
(b) Employment, social security, and social protection	Yes
(c) Vital interests	No
(d) Not-for-profit bodies*	No
(e) Made public by the data subject**	No
(f) Legal claims and judicial acts	No
(g) Substantial public interest conditions	Yes
(h) Health or social care	Yes
(i) Public health	Yes
(j) Archiving, research and statistics	Yes

* Not-for-profit bodies does not include local councils.
** Data is only considered public if the individual deliberately made it so, and intended it would be visible to everyone. Simply being in the public domain is not enough.

See the **ICO guidance** for more information on the additional conditions to process.

Example of a special category data in practice:

A councillor lists their role on a church council in their Register of Interests, which reveals their religious belief;

• Lawful basis: Legal obligation - the council is required by law to publish the register.
• Additional condition (special category data): Substantial public interest conditions - Statutory and government purposes.
• Appropriate Policy Document required: Yes - the council must have an APD

Don't panic if special category data appears in your map. It's common and manageable. You just need to make sure you record it and have the right conditions in place.

3.5 Updating your Data Map

Go back to your data map (Stage One) and add two more columns. For each purpose you've already recorded, note the lawful basis for processing under data protection law (**Article 6**) and, if you are processing special category data, the additional condition that allows it (**Article 9**).

Example of an updated data map:

Purpose of processing	Categories of personal data	Categories of recipients (sharing)	Categories of Processors (data processors on behalf of data controller)	Names of third countries or international organisations that personal data are transferred to (if applicable)	Retention schedule	Article 6 lawful basis for processing personal data	Article 9 condition for processing special category data
Minutes	Identity, Contact information	N/A	Cloud storage provider, Website provider	European Union	Indefinite	Legal obligation	N/A
Accounts	Identity, Contact information, Bank Details	HMRC	Accounts software provider, Cloud storage provider,	European Union	X years after current year	Legal obligation	N/A
Correspondence and Casework	Identity, Contact Information, Special category data	Other Local Authority, Law enforcement and similar competent authorities	Cloud storage provider,	European Union	X years after completion of matter	Public Task	Substantial public interest conditions
Payroll and Pensions	Identity, Contact information, Bank Details	HMRC, pension provider	Accounts software provider, Cloud storage provider,	European Union	X years after current year	Legal obligation	N/A
HR files	Identity, Contact information, Special Category Data	N/A	Cloud storage provider, HR consultants	European Union	X years after employment ends	Contract	Employment, social security, and social protection

3.6 Checklist

- Every purpose in your data map has a lawful basis recorded.
- Where special category data rows have been identified, you have recorded:
    - a lawful basis for processing, and
    - an additional condition to process, and
    - there is an APD if the condition requires it.
- Where consent is used as the lawful basis, individuals have a genuine choice and can withdraw consent at any time.
- You can explain each lawful basis in plain English to a resident.

3.7 Top tip

- If you have an APD, add a link or reference to the relevant row of your data map. This makes key documents easy to find when needed.

3.8 Time to reflect

Consider the following questions as part of your data mapping process, giving regard to the data protection principles of lawfulness, purpose limitation, and accountability:

- Is our processing lawful, and can we point to a law, duty, or function that makes processing all the data necessary?
- Are we abiding by the requirements of each lawful basis and additional conditions to process special category data?
- Would an individual understand the lawful basis for processing their data?
- If we rely on consent, how will we record it and make it easy for people to withdraw it?
- Are we confident that data is only used for the purposes we originally identified, and not for unrelated activities?
- Does our data map truly reflect how we process personal data in practice?

3.9 Summary of outputs from Stage Two

By the end of this stage, your council should have:

- An accurate data map with lawful bases recorded for every purpose.
- Awareness of any special category data and additional conditions to process.
- A solid foundation for Stage Three (risk management).

4 Stage Three

4.1 Goal OF Assessing risks

Protect the rights and freedoms of individuals by identifying risks in your processing activities and putting measures in place to reduce them.

4.2 Why this matters

Data protection law is not about stopping councils from using personal data; it's about using people's data with care and making sure rights and freedoms are respected. Risks might include: breaches of data confidentiality, data being inaccurate or used unfairly, or individuals not being able to exercise their rights under data protection laws.

By assessing risks, councils can reduce the chance of harm to individuals, avoid complaints, and prevent queries being raised with the ICO. To manage risks effectively, make it a habit to consider privacy from the outset of any new activity, project, or system change. This approach is known as privacy by design, and should be a routine part of council business.

Not every risk can be eliminated completely. Councils should reduce risks as much as possible, and then decide what level of residual risk is reasonable based on their size and functions, balancing people's rights with council needs and duties. Each council's appetite for risk will be unique to them and will influence the risk mitigations put in place.

4.3 People's rights under data protection

Individuals have legal rights over their personal data, as set out in **UK GDPR Articles 13** to 23. Councils don't need to be experts, but they do need to recognise these rights and be ready to respond. In short, people have the right to:

- Be informed — To know how and why their data is used, what their rights are and how they can complain.
- Request access — To request a copy of their data (Subject Access Requests).
- Request rectification — To have inaccurate or incomplete data corrected.
- Request erasure — To request deletion of their data in certain situations.
- Request restriction — To limit how data is processed.
- Request data portability — To have their data transferred to another data controller.
- Object — Individuals can object to how their personal data is used. If they are not satisfied with the response, they can raise their concern with the ICO, or in some cases, take it to court.
- Request review of automated decisions — Not to be subject only to decisions made by computers (including profiling) if the decision has a negative effect. They can ask for such decisions to be reviewed by a human.

Fulfilling rights is a legal duty, and not a matter for democratic decision-making. Councils do not have a choice about whether to grant rights, and councillors cannot vote to restrict, refuse or delay them. In practice, rights requests should be handled promptly by a council officer. This ensures compliance and avoids unnecessary meetings or delays.

Most requests to parish councils will be about access, accuracy, or deletion. These can usually be managed with good record-keeping.

See the **ICO guidance** on the rights of individuals.

4.4 Building a practical approach to risk assessment

Parish and town councils don't need complex systems to manage data protection risks; just simple, proportionate steps that show you've thought about people's rights and freedoms. A risk assessment is simply asking what could go wrong, who would be affected, and how serious it would be. The aim is not to eliminate every risk, but to understand it, record your decisions, and put sensible measures in place. This thinking should be done for all the purposes you identified in your data map.

The formal tool for this is a Data Protection Impact Assessment (DPIA). The ICO only requires DPIAs for activities that are likely to be high risk, but in practice, you often don't know something is high risk until you start looking at it. That's why it helps to treat DPIAs as a routine part of managing personal data.

A light-touch risk review:

For most day-to-day activities, a short review is enough to show that you've considered privacy and security. Ask yourself:

- What could go wrong?
- Who might be affected?
- How serious would it be?
- What can we do to reduce the risk?

This simple approach follows the same principles as a DPIA. Writing down your answers, even briefly, shows accountability and helps you spot where extra safeguards are needed.

Full DPIA for higher risk, or changing activities:

When something is new, involves more personal data, or feels sensitive (such as introducing CCTV, running a community survey, or launching a new website), complete a full DPIA. It's simply a more detailed version of the same thinking process. The key steps are:

- Describe what you plan to do.
- Identify whose data is used and what risks can arise.
- Plan safeguards to reduce those risks.
- Record your reasoning in writing.

A DPIA doesn't need to be long or complicated; it just needs to show that you've thought about the impact on people's privacy and taken proportionate action. The ICO has a **downloadable DPIA template** you can follow.

Why this approach works:

This staged approach builds data protection into everyday council work. Light touch reviews keep things simple and consistent, while full DPIAs give deeper assurance where the risks are higher. Together they make risk assessment realistic and achievable for councils of all sizes, and keep the focus where it should be - on protecting people's rights.

To see how this works in practice, the following example shows the four steps applied to a common council activity - taking photos at an event. It demonstrates that risk assessment doesn't need to be complex; it just needs to be thoughtful, proportionate, and clearly recorded.

4.4.1 Example DPIA for council event photography

This example shows how a parish council could complete a Data Protection Impact Assessment (DPIA).

- Describe what you plan to do — The council wants to take photographs at community events for publicity purposes, and use images on its website, newsletters, and social media channels, to provide feedback to the community on event success. The lawful basis will be legitimate interest. Photos will be stored in the council's cloud account and kept for no longer than 20 years unless they are judged historically significant.
- Identify whose data will be used and risks that could arise — Photos will include members of the public (sometimes children or vulnerable people).
    - Risks: People may not want their photo taken (medium risk).
    - Loss of data if equipment is lost or stolen (low risk).
    - Loss of data if the equipment is damaged. (low risk).
- Plan safeguards to reduce risks:
    - Post clear signs at event entrances to say photos will be taken. (reduces risk (i)).
    - The photographer is to wear a high-visibility vest so people can avoid or ask not to be included. (reduces risk (i)).
    - Where only one or two people are in shot, seek consent. (reduces risk (i)).
    - Risks ii. and iii. are acceptable to the council and do not need mitigating.
- Record your reasoning in writing:
    - Record risks and mitigations.
    - The clerk has signed off on the DPIA.
    - Review regularly.

See this example modelled on the ICO template ***<link to downloadable doc>***.

4.5 Working with data processors

UK GDPR Article 28 requires data controllers to have formal contracts with any organisation or person (data processor) that handles data on their behalf. Having a contract in place ensures you and the processor follow data protection laws, keep personal data secure, and understand who is responsible for what.

A written agreement is essential whenever you hire a processor to work with your personal data, and often forms part of their terms and conditions. When creating a contract, make sure it includes:

- Processing only on the documented instructions of the controller.
- Duty of confidence.
- Appropriate security measures.
- Using sub-processors.
- Data subjects' rights.
- Assisting the controller.
- End-of-contract provisions.
- Audits and inspections.

When working with data processors, it's essential to assess each one on a case-by-case basis. Make sure you're comfortable, and there is an adequate contract in place before engaging their services.

4.6 International transfers: when council data leaves the UK

When personal data leaves the UK, people's rights can be affected. Other countries may not have the same data protection safeguards, which increases the risk of the council being unable to comply with individuals' rights. By checking where data goes and choosing lower-risk transfer options, councils are protecting personal data.

International transfers are not rare or unusual. Many everyday tools used by councils (like cloud-based storage, email, newsletter platforms, or design apps) rely on servers outside the UK. That's why it's important to check where your data is stored and make sure the right safeguards are in place.

There are three main situations if your data leaves the UK:

- Data stored in the EU and adequate countries (lowest risk) — Data kept in the EU (or any country on the UK's **adequacy list** is safe. These countries have strong data protection laws, so no extra action is required other than noting the transfer in your documentation.
- Data stored in the USA (higher risk) — Councils can use USA companies if they are certified under the official UK extension to the EU-USA Data Bridge Scheme. You must check that the company is on the **US government's list**. If they are not certified, then this approach is not valid, and you will need to use an International Data Transfer Agreement instead.

- Data stored in all other places (Very high risk) — If data is transferred to counties outside the adequacy list or the USA scheme, councils must use **International Data Transfer Agreements** (IDTA). Before proceeding, councils should risk assess each IDTA on a case-by-case basis, considering the residual risk and any additional safeguards required. Only proceed if mitigated risks are at an acceptable level.

4.7 Top Tip

Always choose the simplest and safest option available. Where possible, select providers that keep data in the UK, EU, or adequate counties. If that isn't possible, be ready to evidence your decision-making and ensure you are content with the residual risks that remain.

4.8 Checklist

Have you considered the following risks?

- Is data stored securely (For example, locked cabinets, password protection, multi-factor authentication, up-to-date computer equipment, etc)?
- Is data held on personal devices?
- Is the data correct and kept up to date?
- Is data kept longer than needed?
- Are data processors used (i.e. payroll providers, website hosts, IT support)?
- Are there contracts in place with them?
- Is the data published online?
- Is data transferred internationally?
- Can individuals exercise their rights easily if they ask?
- Can requests for access, rectification, or deletion be handled appropriately?
- Are new or changing systems (websites, apps, surveys) being risk assessed at the start?

4.9 Top tips for updating your data map

Where you have a DPIA, add a link or reference to the relevant row of your data map. This makes key documents easy to find when needed.

4.9.1 Time to reflect

Consider the following questions as part of your risk assessment process, giving consideration to the data protection principles of accuracy, security, and accountability:

- Do we know which types of data carry the biggest risks in our council (e.g. staff data, resident complaints, financial records, special category data)?
- Have we considered how processing activities could affect someone's privacy?
- What measures can we take to reduce the risks associated with our processing, and are we confident they are effective?
- When risks can't be removed, have we identified and documented residual risks, and are we clear why we accept them?
- How do we ensure the accuracy of personal data, and what processes are in place to correct or update data when necessary?
- Are all councillors and staff aware of their role in reducing risks?
- If we were asked about how we protect personal data, could we explain it simply?

4.10 Summary of outputs from Stage Three

By the end of this stage, your council should have:

- A written record of your key risk decisions, ready to feed into Stage 4 (policies):
    - An assessment of risks linked to each purpose identified on your data map.
    - Notes on what mitigations you will use (or why you accept certain risks).
- Understanding that privacy is now a key consideration at the beginning of new projects.
- A culture of viewing data protection as protecting people's privacy and rights, not just paperwork.

5 Stage Four

5.1 Goal of Policies, procedures and training

Turn your council's decisions about data protection into clear information and apply them to your everyday working practices.

5.2 Why this matters

Mapping your data (Stage One), identifying lawful bases (Stage Two), and assessing risks (Stage Three) have helped you understand what data you hold, why you use it, and where risks may arise. This stage turns all that work into action by putting your council's decisions into clear words and repeatable steps.

Policies, procedures, and training are what make good intentions part of daily practice. They help officers and councillors work consistently, give confidence when things go wrong, and provide assurance to individuals that their information is being handled properly.

Think of this stage as the bridge between planning and doing, where data protection becomes part of your council's routine operations.

5.3 Where to start

If you've followed the previous stages, you already have most of what you need. Your data map shows what personal data you process and why; your lawful bases tell you the legal grounds, and your risk assessments help you identify safeguards.

Now, it's time to bring all that together into:

- Policies — To set the rules and expectations for councillors and staff.

- Procedures — To guide daily tasks and ensure consistency.
- A privacy notice — To explain your data use to the public.
- Training — To build confidence and awareness across the council.

Don't worry about getting everything perfect right away. Start with simple, clear documents that reflect how your council actually works, and build from there.

5.4 Policies: Setting the rules

Policies are your council's internal rulebook for managing personal data. They ensure everyone (councillors and staff) handles data in the same safe and lawful way.

You don't need a long policy suite. Start with a few clear, practical ones that match your data map and risk assessments. Each policy should:

- Reflect the purposes and risks you've identified.
- Be simple and easy to follow.
- Be reviewed regularly to stay up to date.

5.4.1 Data Security Policy

Data security means keeping council information safe, accurate, and only accessible to the right people. Risks often arise when data is moved outside secure council systems, such as onto personal email accounts or devices, where it can be lost or mishandled. A clear Data Security Policy sets the ground rules for how information is stored, shared, and protected. It should align with your council's IT Policy and cover both security measures for your council systems (e.g. passwords, backups, and locked storage) and rules on transferring out of council systems, ensuring everyone works consistently, protects individuals' privacy, and makes it easier to handle data requests or breaches. Your policy should cover:

- Responsibility — Who oversees data security (usually the clerk).
- Passwords — Minimum requirements and confidentiality.
- Multi-factor authentication — When and how it's used.
- Physical security — How paper files, keys, and devices are stored.
- Access control — Who has access to different files or systems?
- Backups — How and how often data is backed up.
- Deletion —Gow data is securely erased when no longer needed.
- Bring your own device - whether personal devices can be used for council work, and any restrictions if they are, such as:

- Email — Which email systems can be used for council data?
- Storage — Which cloud platforms are authorised (e.g. OneDrive, SharePoint)?
- Restrictions — Whether downloading council files to personal devices is allowed.
- Equipment — Does the council provide devices, or can personal ones be used?
- Instant messaging/social media – rules on using WhatsApp, Facebook, or similar platforms for council business.

Top tip:

- Make sure your Data Security Policy works hand in hand with your IT Policy — both should set out consistent rules for keeping information safe, whether it's stored digitally or on paper.

5.5 Data Breach Policy

This policy helps your council to respond quickly and confidently if something goes wrong (e.g. lost laptop, email sent in error, hacking attempt). Having a plan in place means less stress, compliant action, and faster recovery if a breach ever occurs. Your policy should include:

- Definition — What counts as a data breach (loss, unauthorised access, damage to data).
- Responsibility — Who leads the response (usually the clerk).
- Reporting — How councillors and staff should report any suspected breach.
- Timescales — Key actions within the 72-hour window.
- Escalation — Who is authorised to try to fix issues, and when to notify the ICO.
- Record keeping — How breaches are documented to support learning and improvement.

5.6 Rights Requests Policy

This policy explains how the council handles requests from individuals to exercise their legal rights (e.g. access, correction, deletion). Your policy should cover:

- Identification — What counts as a request, including various forms such as verbal communications, informal emails, and letters, without the need for a form.

- Rights — Identify the types of rights, e.g. access, rectification, erasure, etc.
- Responsibility — Who manages requests (usually the clerk).
- Reporting — How councillors and staff should pass requests on.
- Content — What information to provide in a Subject Access Request.
- Erasure — When deletion requests may be refused (e.g. where law requires records to be kept).
- Timescales — One calendar month to respond (the legal deadline).
- Escalation — How individuals can complain if unhappy (e.g. complaints policy or ICO).

5.7 Putting policies into action

Once council policies are in place, it is the council's officers who will put them into practice day to day - handling requests, maintaining records, and making sure the right steps are followed. Councillors don't need to decide each case individually; the policy provides the framework.

While a formal Data Protection Officer is not required for most parish councils, every council should appoint a responsible officer (usually the clerk) for data protection matters. This provides a clear point of contact, clarifies accountability, and keeps everything running smoothly.

It is important to ensure your designated officer is adequately supported to perform their data protection responsibilities. Data protection matters can arise at any time, and often have strict timescales which can impact an officer's workload (especially a clerk). Officers will require time, tools, and training to carry out these tasks effectively. Adequate resourcing ensures the council remains compliant, as well as protecting the officer from undue pressure.

5.7.1 Procedures: turning policy into practice

Procedures are the how-to guides that help everyone follow policies consistently. They should be short, practical, and tailored to your council. Examples include:

- Handling emails safely (e.g. always using Bcc for group emails).
- Responding to access requests (log, track, and respond on time).

- Managing paper records (secure storage, key access, shredding).
- Using cloud systems (checking provider contracts, passwords, and backups).

Procedures don't have to be formal documents. A short checklist or flowchart can work just as well. The aim is consistency, so that anyone new to the council can follow the same steps confidently.

5.7.2 Privacy Notices: Being open and transparent

A privacy notice is a legal requirement. It's the council's public-facing document that tells people what you do with their personal data, why you need it, and how they can exercise their rights. A good privacy notice builds trust and shows transparency.

It can be tempting to write your privacy notice first, but without the groundwork from Stage One to Stage Three, it will be incomplete or inaccurate. That's why writing the privacy notice comes at the end of the process - it draws everything together.

A privacy notice should feel like a clear, informative guide, and not a legal contract. If people can read it once and explain it back to you, you're on the right track.

Where to start with your privacy notice:

Begin with your data map. Every purpose listed there will appear in your notice, along with its lawful basis, sharing, retention, and any special category data.

A privacy notice is a legal requirement. It is a public-facing document that tells people what you do with their personal data, why you need it, and how they can exercise their rights. It's also a chance to build trust by showing the council is open and accountable.

It can be tempting to write your privacy notice first, but without the groundwork from Stages One to Stage Three, it will be incomplete or inaccurate. That's why writing the privacy notice comes at the end of the process.

A privacy notice should feel like a straightforward, informative guide, and not a legal contract. If people can read it in one sitting and explain it, you're on the right track.

5.7.3 Checklist on what to include in your privacy notice

In plain English, your notice should explain:

- Who you are — The name of the council, and how people can contact you.
- Why do you use data — List each purpose (yes, every one from your data map), e.g. publishing minutes, managing payroll, handling correspondence.
- Your lawful basis — State which lawful basis applies to each purpose.
- Special category data — Where you process it, state the additional condition you rely on.

- Legitimate interest — If you use it for any purpose, explain what the interest is in each case.
- Who you share data with (Data Controllers) — Name organisations (e.g. HMRC) or describe categories (e.g. Banks).
- Who processes data for you (Data Processors) — Name organisations (e.g. payroll provider) or describe categories (e.g. auditors).
- International transfers — Explain if data leaves the UK and what safeguards are in place (e.g. adequacy decision, UK extension to EU-USA Data Bridge Scheme, or an International Data Transfer Agreement).
- Retention — Say how long you plan to keep personal data for each purpose.
- Consent — Where you rely on consent as your lawful basis for any purpose, explain that people can withdraw it at any time and how they can do so.
- Complaints — Tell people how they can complain to you, and to the ICO.
- Automated decisions — If you make any, explain what they are and their effects on people.
- Rights — Explain the eight data protection rights in plain English (you can use the ICO's template wording).

5.7.4 Top tips for drafting your privacy notice

- Keep it clear and jargon-free. Imagine explaining it to a resident at a parish meeting.
- Don't copy another council's notice. Remember, every council processes data differently.
- Use the **ICO's template** as a guide. It includes suggested wording for rights and complaints.
- Publish it where people can find it easily, i.e. your website or noticeboard.
- Consider short just-in-time notices at the point of data collection (e.g. on forms, surveys, CCTV signs, or event sign-ups). These briefly explain why data is being collected and can link to your full privacy notice.

5.7.5 Training: Building confidence

Councillors and staff don’t need to be data protection experts, but they do need to:

- Understand the basics of personal data and people’s rights.
- Know their responsibilities as part of the council.
- Feel confident about what to do if something goes wrong.

Training can be simple:

- A short induction for new councillors.
- Short courses and annual refreshers for council officers.
- Sharing ICO resources or NALC and county association guidance.

The key is to make training relevant and practical, showing how data protection applies to the council's real activities.

5.8 Checklist

- Are policies written, approved, and consistent with our data map and risks?
- Do councillors and staff know how to report a data breach?
- Is there a simple, reliable process for rights requests (e.g. Subject Access Request)?
- Do we have a clear, up-to-date privacy notice published where people can find it?
- Have all councillors and staff received basic data protection training, with refreshers planned?

5.8.1 Time to reflect

Consider the following questions as part of embedding practices, giving consideration to the data protection principles of lawfulness, transparency, and accountability:

- Are we being open and transparent about the data we process?
- Would everyone in the council know what to do if a resident asked for their data?
- Are our policies and procedures practical enough for people to actually follow them?
- Could we confidently explain our approach and decisions if questioned?
- Is training seen as an ongoing part of good governance, rather than a one-off event?

5.9 Summary of outputs from Stage Four

By the end of this stage, your council should have:

- Core data protection policies tailored to your council's work.
- Simple procedures that councillors and staff can follow.

- A published privacy notice.
- Training is in place for councillors and staff.
- A growing culture of awareness, where everyone understands their part in protecting people's data.

6 Reviewing

6.1 Goal OF MONITORING AND REVIEWING

To maintain strong and consistent data protection practices.

6.2 Why this matters

Data protection is not a one-off task. Councils change over time; new services are introduced, staff or councillors change, and technology moves on. A system that works today may not be fit for purpose tomorrow. Regular monitoring and review help keep your council compliant, confident, and able to respond to new challenges.

6.3 Monitoring your data protection practices

Day-to-day monitoring is about keeping data protection active and visible in your council's routine work. Your data map should remain the central record and be updated whenever something changes, e.g. if the council introduces a new service, takes on a new provider, or starts handling a different type of data. This keeps your records accurate and prevents issues later.

If a new purpose for processing data is identified at any point, ensure data protection is considered from the start, and carry out a Data Protection Impact Assessment (DPIA). And don't forget to update your privacy notice too.

Your council's policies will only work if they are followed in practice. Simple spot-checks can help the council see whether its rules are working as intended. For example, you might check whether councillors are using their council email accounts rather than personal ones, whether paper records are stored securely in locked cabinets, or whether retention schedules are being applied when information is no longer needed. These checks should not feel punitive; they are a way of catching small issues early, and before they turn into bigger problems.

How spot-checks can help:

Imagine your council has several filing cabinets and archive boxes filled with paper files dating back many years. Likelihood is that there is never time to go through them, shred them, and it's just piling up.

One day, someone submits a subject access request, asking to see their personal data. Suddenly, you're faced with the daunting task of searching through all those files to find the relevant information. You can't shred them now that the request has been made. This has now become a costly, time-consuming task which could have been avoided with better data management.

A simple spot check could have highlighted the risk of non-compliance with data protection principles (data minimisation, storage limitation, security, and accountability). A regular review of data stored on site could have highlighted the accumulation of unnecessary files and associated risks, and prompted action, including prioritisation and resource allocation to the task. This could have prevented what is now a significant use of officer time, which could have been spent elsewhere.

Keeping a log of rights requests, such as Subject Access Requests or requests for deletion, helps the council monitor how well it is meeting its legal duties. The log can show whether requests were handled within the one-month time limit, whether responses were clear, and whether any delays or difficulties occurred. Looking back at this record periodically provides reassurance that the council is handling requests consistently and can also highlight areas where further resources, training or clearer processes might be helpful.

It is easy to assume that everyone will know what to do in the event of a data breach, but practice often tells a different story. Running a simple exercise, for example, by asking 'what would we do if an email with resident details was sent to the wrong person?', can be very effective. These tests highlight who would take the lead, what timescales apply, and where the process might be unclear. By rehearsing scenarios, the council builds confidence that it can respond quickly and lawfully if a real breach occurs.

It is important that councillors and staff understand their role in protecting data. New staff and councillors would benefit from data protection training as part of their induction. Periodic refresher sessions will remind them of their responsibilities and build confidence in handling data effectively.

Mistakes happen, so encourage a culture where potential issues are raised quickly and without blame. Don't panic if you have a data breach; even the best compliance council can have something go wrong. If someone suspects a data breach or receives an unusual request, it should feel normal to report it straight away. This ensures problems are dealt with early and demonstrates that the council takes its duty of care seriously.

6.4 Reviewing regularly

Councils should plan to review their data protection arrangements regularly. Choose a review cycle that is achievable and reflects the council's size, scale of processing, and resources. For most parish councils, an annual review is a sensible starting point. Smaller councils may prefer to do this alongside their AGAR preparations, as part of their Annual Meeting, or at another convenient point in the year. The key is to make reviews a routine part of your governance.

At review, check:

- Is the data map still accurate?
- Are your policies up to date and being followed? Has any guidance changed?
- Have DPIAs taken place for new or changed activities?
- Are retention periods being applied in practice?
- Have any rights requests been handled properly and on time?
- Are contracts with processors still valid and clear?
- Is the privacy notice still accurate?

Make notes of each review in your council minutes or internal records to show that it has taken place and what was discussed or updated. This demonstrates accountability and provides evidence, if ever needed, that the council actively monitors its data protection compliance and that a substantial review has been undertaken.

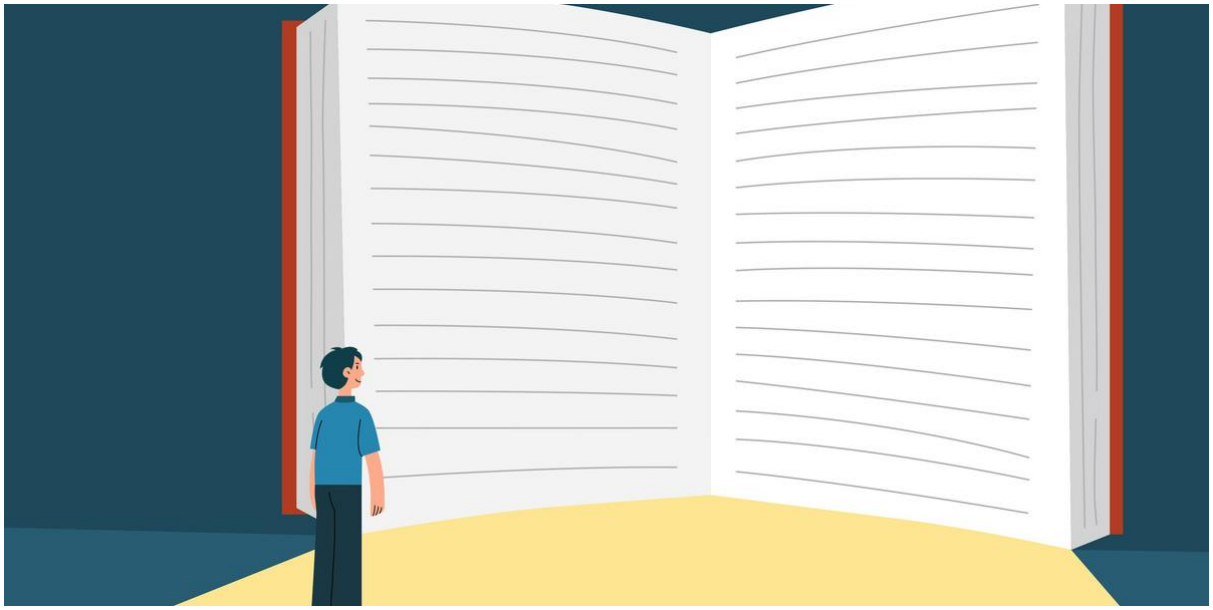
6.5 Top tips for continuous improvement

- Treat every rights request, breach, or query as an opportunity to learn. Ask: What went well? What could we improve? Did we have adequate resources?
- Keep an eye on updates from the ICO, NALC, or your county association — laws and guidance do evolve.

- Consider small improvements each year, such as introducing stronger passwords, minimising records, or software and systems improvements.

By making monitoring and review part of your routine, your council will:

- Keep compliance up to date without needing a major or costly overhaul.
- Build confidence among councillors, staff, and residents.
- Create a culture where data protection is seen as part of good governance, not extra or token paperwork.



7 Principles

7.1 Understanding data protection principles

Data protection might sound complicated, but at its heart, it's simply about handling people's personal information responsibly and respectfully. For councils, this means thinking carefully about the information you collect and process, and ensuring people's legal rights can be met.

The law is based on seven key principles, which guide everything you do with personal data:

7.1.1 Lawfulness, fairness, and transparency

Every time you collect personal information, you need to be clear about why you are doing it. We call these reasons purposes. For each purpose, you must have a lawful basis, a valid reason allowed by law to use the data. Once you have a lawful basis, you must stick to it. People should know what information you are collecting and why. Your use should be transparent and fair.

7.1.2 Purpose limitation

You must say why you need the personal data when you collect it, and you must only use personal data for the reason you collected it. For example, if you collect names and contact details to run an allotment, you cannot then use that same data for an unrelated activity, such as a youth club fundraising event. The purpose you identify to collect data sets the boundary for how you use the information.

7.1.3 Data minimisation

Collect only what you need for your stated purpose. Don't ask for extra information that isn't relevant. For instance, when managing allotments, you don't need to know a person's marital status or sexual orientation; it's irrelevant! Keeping data limited to what is necessary reduces risks and makes management easier.

7.1.4 Accuracy

Ensure the information you hold is correct and up-to-date. Small errors can cause big problems. Simple steps, like confirming email addresses when people sign up for updates, can help keep your records accurate. Regular reviews of your data help make sure it remains reliable.

7.1.5 Storage limitation

Personal data should only be kept for as long as it is needed for its purpose. Once the work is done, like a completed consultation or project, review the data and remove what is no longer necessary. This principle helps prevent unnecessary data piling up. Do not keep data 'just in case' it might be useful later.

7.1.6 Integrity and confidentiality (security)

Protect personal information from loss, damage, or misuse. This includes digital security, physical records, and even video or recorded speech if it can identify someone. Security isn't just about malicious hackers; accidents like deleting files and data corruption also count. Ensure you have measures in place to keep all types of data safe.

7.1.7 Accountability

Finally, you must be able to show that you are following these principles. Keep records of what data you hold, why you hold it, and the decisions you make to protect it. This includes a data map (an overview of the data you process), risk assessments, and clear policies and procedures to guide everyone in the council. Being accountable isn't just good practice; it streamlines council operations and builds trust with the community.

In short, data protection is about being responsible with the information people trust you with, and transparent about how you use it. By following these principles, your parish council can protect people’s personal data, comply with the law, and operate efficiently and safely.

8 Glossary

Appropriate Policy Document (APD) A short written document that explains how the council will protect and manage special category data. It must describe how you comply with the data protection principles and how long you keep information.

Data Breach An incident where personal data has its confidentiality lost, its integrity damaged, or its availability removed — whether by accident or on purpose. Data breaches can vary significantly in scale, from small incidents to major catastrophes. It is essential for councils to maintain records if them to identify patterns and prevent future errors.

Data Controller A person or an organisation that decides why and how personal data is used. The council will be a data controller, and it's common for councils to share data with other data controllers, e.g. passing employee payroll data to HMRC.

Data Map A record of processing activities (often a table or spreadsheet) that sets out what personal data the council holds, why it is used, where it is stored, who can access it, and how long it is kept. The detailed and well-thought-out data map is the foundation for all other data protection work.

Data Processor An external company or person that processes personal data on the council's behalf, but does not decide how it is used. Examples include email providers, payroll providers, website hosts, or cloud storage companies. Councils must have a written contract in place with processors that set outs requirements and obligations to comply with data protection law.

Data Protection Impact Assessment (DPIA) A structured risk assessment that helps the council think through how an activity affects people’s privacy, what risks might arise, and what mitigations can be put in place to reduce the risks identified.

Data Protection Officer A data protection officer (DPO) is a formal position appointed for compliance monitoring, providing independent advice, and acting as a contact point.
Parish councils are normally exempt from the requirement to appoint a DPO. Note: In rare cases where a parish council is regularly monitoring individuals or undertaking large-scale processing of special category or criminal convictions data, then a DPO may still be required.

Data Subject Any individual whose personal data is being processed. This could be anyone, including staff, councillors, contractors, and residents.

Personal Data Any information that identifies a living person, either directly (e.g. name) or indirectly (e.g. job title, reference number, or photo). Ask yourself, can this information identify who the person is? If yes, it's personal data.

Processing Anything you do with personal data, including collecting, using, storing, sharing, publishing, or deleting it. If you handle personal data in any way, you are processing it.

Purpose The reason personal data is being used. Examples include (but are not limited to) keeping minutes, paying staff, or running an allotment. A council will have multiple different purposes.

Special Category Data A type of personal data that is more sensitive and needs extra protection. It includes personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health, sex life and sexual orientation.

Lawful Basis The legal reason for processing personal data under the UK GDPR (Article 6). Every purpose in your data map must have a lawful basis assigned to it and recorded.

Privacy Notice A single public-facing document, tailored to the council, that explains in plain English what personal data the council processes, why it is used, how long it will be kept for, how to complain and what rights people have.

Rights Requests Requests made by individuals to exercise their data protection rights, such as access, correction, or deletion. Requests can be made to the council verbally or in writing, without the need to contact a specific person or use a form. These requests must be dealt with by the council promptly and within a timeframe of usually one month.

+++END+++