ST ATHAN COMMUNITY COUNCIL
UK GDPR AND DATA PROTECTION POLICY

Adoption

Adopted by St Athan Community Council at the Full General Council meeting held on Tuesday 7th July 2026 and replaces the former General Data Protection (GDP) Policy.
Version: 2.0.

Minute reference: 3504
Review date: May 2027

Signed:
Name:
Chair of St Athan Community Council

Note: This policy is written for Council use in England and Wales data protection terms. It should be read alongside the Council's privacy notices, records retention schedule and complaints policy adopted by the Council.

1. Purpose

1.1 This policy sets out how St Athan Community Council will comply with data protection law when collecting, using, storing, sharing, retaining and disposing of personal data.

1.2 The Council handles personal data in order to carry out its statutory functions, manage its services, employ staff, pay suppliers, administer meetings, communicate with residents, manage events and facilities, respond to enquiries and complaints, and meet legal and audit obligations.

1.3 The Council is committed to protecting personal data and ensuring that individuals are treated lawfully, fairly and transparently.

2. Scope

2.1 This policy applies to all personal data processed by or on behalf of the Council, whether held electronically, on paper, in emails, on websites, in photographs, in recordings, in minutes, in finance systems or in any other format.

2.2 This policy applies to councillors, employees, volunteers, contractors, consultants and any person who processes personal data on behalf of the Council.

2.3 This policy covers personal data relating to employees, councillors, job applicants, contractors, suppliers, hall or facility users, event participants, volunteers, residents, complainants, correspondents, website users and any other person whose personal data is processed by the Council.

3. Legal framework

3.1 The Council will comply with the following legislation and regulatory requirements, where applicable:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018;
- the Data (Use and Access) Act 2025, including relevant amendments to UK data protection law;
- the Privacy and Electronic Communications Regulations 2003 (PECR), where electronic communications or direct marketing are relevant;
- the Freedom of Information Act 2000 and Environmental Information Regulations 2004, where information requests involve personal data;
- employment, local government, audit, health and safety, safeguarding and equality legislation, where these require or justify processing personal data.

3.2 The Data (Use and Access) Act 2025 has introduced phased changes to data protection law. This policy includes the new requirement for organisations to have a data protection complaints process, which is due to come into force on 19 June 2026.

3.3 This policy does not replace the Council's privacy notices. Privacy notices must explain, in plain language, how and why the Council processes personal data in particular circumstances.

4. Key definitions

Term	Meaning
Personal data	Information relating to an identified or identifiable living individual.
Special category data	More sensitive personal data, including information about health, race or ethnic origin, political opinions, religion or belief, trade union membership, genetics, biometrics, sex life or sexual orientation.
Criminal offence data	Information relating to criminal convictions, offences, allegations or related security measures.
Processing	Anything done with personal data, including collecting, recording, using, sharing, storing, deleting or destroying it.
Data subject	The individual the personal data relates to.
Controller	The organisation that decides why and how personal data is processed. For Council business, St Athan Community Council is normally the controller.
Processor	A person or organisation that processes personal data on behalf of the Council, such as an IT, payroll, website or cloud service provider.
Personal data breach	A security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. Data protection principles

5.1 The Council will comply with the UK GDPR data protection principles. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary;
- processed securely, using appropriate technical and organisational measures;
- managed in a way that enables the Council to demonstrate accountability.

5.2 Accountability means that the Council must not only comply with data protection law, but must also be able to show how it complies. This includes keeping appropriate records, policies, privacy information and decision notes.

6. Roles and responsibilities

6.1 St Athan Community Council is the data controller for personal data processed for Council business. Individual employees, councillors and contractors must follow this policy when acting for or on behalf of the Council.

6.2 The Proper Officer is responsible for day-to-day coordination of data protection compliance, including maintaining records, handling rights requests, coordinating breach response and ensuring that privacy notices and retention arrangements are kept under review.

6.3 The Responsible Financial Officer is responsible for ensuring that finance, payroll, audit, banking, supplier and accounting records are processed securely and retained in line with legal and audit requirements.

6.4 Councillors must protect personal data they receive through Council business, use it only for proper Council purposes, and must not disclose it without lawful authority.

6.5 Employees, volunteers and contractors must report any suspected personal data breach, data loss, unauthorised disclosure or data protection concern to the Proper Officer as soon as possible.

6.6 Community councils are not generally treated as public authorities for the UK GDPR Data Protection Officer requirement. The Council may appoint a Data Protection Officer or external data protection adviser voluntarily, but this does not remove the Council's responsibility as controller.

7. Lawful bases for processing

7.1 The Council must identify a lawful basis before processing personal data. The most likely lawful bases for Council processing are:

Lawful basis	Council example
Public task	Processing necessary for the Council to perform public functions, administer council business, respond to residents, manage meetings and deliver services.
Legal obligation	Processing required by law, including employment law, audit requirements, tax, accounting, health and safety, equality duties and statutory publication duties.

Contract	Processing necessary to enter into or perform a contract, such as employment, service contracts, facility bookings or supplier arrangements.
Legitimate interests	Only where appropriate and not where the Council is processing as a public authority carrying out public tasks.
Consent	Used only where the person has a genuine free choice, for example optional publicity photographs or optional non-statutory communications. Consent must be specific, informed and capable of being withdrawn.
Vital interests	Used only where processing is necessary to protect someone's life or safety in an emergency.

7.2 The Council will not rely on consent where another lawful basis is more appropriate. Council meeting administration, employment, audit, statutory correspondence, payment of allowances and legal compliance should not normally depend on consent.

7.3 Where consent is used, the Council will keep a record of what the person consented to, when they consented, how they consented, and how they may withdraw consent.

8. Special category and criminal offence data

8.1 The Council will process special category data only where there is a lawful basis under Article 6 UK GDPR and a separate condition under Article 9 UK GDPR and, where required, the Data Protection Act 2018.

8.2 Special category data may arise in employment records, sickness absence, reasonable adjustments, equality monitoring, safeguarding, complaints, incident reports, grant applications, community events or correspondence from residents.

8.3 Criminal offence data will only be processed where necessary, lawful and proportionate, and where a condition under the Data Protection Act 2018 is met.

8.4 Where required by the Data Protection Act 2018, the Council will maintain an appropriate policy document setting out its retention and erasure arrangements for special category or criminal offence data processed under relevant conditions.

9. Personal data held by the Council

9.1 The Council may hold the following types of personal data, where necessary and proportionate:

- names, addresses, email addresses, telephone numbers and contact preferences;
- employment, recruitment, payroll, pension, tax and training records;
- councillor contact details, declarations of interest, attendance and allowance records;
- supplier, contractor, grant applicant, hirer and event participant information;
- bank details and payment records where needed for lawful payment administration;
- correspondence, complaints, enquiries and service request information;
- photographs, video or audio recordings where lawfully obtained and necessary;
- website, social media or electronic communications data where relevant;

- health, accessibility or safeguarding information where necessary for employment, events, safety, welfare or legal compliance.

9.2 The Council will avoid collecting personal data “just in case”. It will collect only what is needed for a defined purpose.

10. Privacy notices and transparency

10.1 The Council will provide privacy information to individuals at the point their personal data is collected, unless an exemption applies.

10.2 Privacy notices should explain:

- the identity of the Council as controller and relevant contact details;
- the purposes for which personal data is processed;
- the lawful basis for each purpose;
- what personal data is processed and where it comes from;
- who personal data may be shared with;
- how long personal data will be kept;
- individual rights and how to exercise them;
- how to complain to the Council and to the Information Commissioner’s Office.

10.3 The Council will keep privacy notices under review, especially when introducing a new service, system, event, project, consultation, recording arrangement or data-sharing arrangement.

10.4 Where the Council records Council or Committee meetings for the purpose of preparing accurate draft minutes, the Council will provide clear privacy information through its Meeting Recording Policy, Privacy Notice and Retention Arrangements. This will explain the purpose of recording, lawful basis, what information may be captured, who may access the recording, how long it will be kept, how it will be securely deleted, and how individuals may raise data protection concerns or exercise their rights.

11. Individual rights

11.1 Individuals have rights under data protection law. Depending on the circumstances and lawful basis, these may include:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure, where it applies;
- the right to restrict processing;
- the right to data portability, where it applies;
- the right to object, where it applies;
- rights relating to automated decision-making and profiling, where relevant.

11.2 These rights are not all absolute. The Council may need to continue processing or retaining information where required by law, audit rules, employment obligations, public task, legal claims, safeguarding or the rights and freedoms of others.

11.3 Requests to exercise rights should be sent to the Proper Officer. The Council will verify identity where necessary and will respond within the statutory timescale.

12. Subject access requests

12.1 A subject access request is a request by an individual for copies of their personal data and other supplementary information. It may be made verbally or in writing, including by email or social media.

12.2 The Council will respond to subject access requests without undue delay and normally within one calendar month of receipt. Where a request is complex or the individual has made multiple requests, the Council may extend the time by up to a further two months, but must tell the requester within one month and explain why.

12.3 If the Council needs to confirm identity or clarify the scope of the request, the timescale may not begin, or may be paused, until the necessary information has been provided.

12.4 The Council will consider whether information about third parties, confidential references, legal privilege, crime prevention, negotiations, management information or other lawful exemptions apply before disclosure.

12.5 Subject access requests must be logged and handled confidentially. Councillors and staff must immediately forward any request they receive to the Proper Officer.

13. Data protection complaints

13.1 A data protection complaint is a complaint about how the Council has handled personal data or complied with data protection law.

13.2 The Council will provide a clear way for individuals to make data protection complaints, including by email, post and, where practical, an electronic form or website contact route.

13.3 The Council will acknowledge receipt of a data protection complaint within 30 days of receiving it, take appropriate steps to consider and investigate the complaint, keep the complainant informed, and provide the outcome without undue delay.

13.4 Data protection complaints should normally be handled by the Proper Officer unless the complaint concerns the Proper Officer, in which case the Chair or another authorised person should coordinate the response while maintaining confidentiality and impartiality.

13.5 If the complainant remains dissatisfied, they may complain to the Information Commissioner's Office. The Council will provide ICO contact information in its privacy notices and complaint responses.

13.6 Data protection complaints may also be considered under the Council's Complaints Policy where appropriate, but statutory data protection timescales and requirements must be observed.

14. Personal data breaches

14.1 A personal data breach can include loss of papers, sending an email to the wrong recipient, unauthorised access, cyber incident, lost device, accidental deletion, ransomware, disclosure in minutes, publishing personal data online, or sharing personal data without a lawful basis.

14.2 All suspected breaches must be reported immediately to the Proper Officer. Delay may prevent the Council from meeting its legal reporting obligations.

14.3 The Council will assess each suspected breach promptly to decide:

- what happened and what data was involved;
- who is affected and what risks may arise;
- what containment or recovery action is needed;

- whether the breach must be reported to the Information Commissioner's Office;
- whether affected individuals must be informed;
- what lessons should be learned to reduce future risk.

14.4 Where a breach is reportable, the Council must report it to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it.

14.5 The Council will keep a record of all personal data breaches, including those not reported to the Information Commissioner's Office, together with the reasons for any reporting decision.

15. Data security

15.1 The Council will use appropriate technical and organisational measures to protect personal data. Measures should be proportionate to the sensitivity, volume and risk of the data held.

15.2 The following controls will be applied where appropriate:

- password protection and multi-factor authentication where available;
- secure storage of paper records and locked cabinets where needed;
- restricted access to files and systems on a need-to-know basis;
- regular software updates and anti-malware protection;
- secure back-up arrangements;
- encryption or password protection for sensitive documents sent electronically;
- careful use of blind-copy when emailing multiple external recipients;
- checks before publishing documents to ensure personal data is not disclosed unlawfully;
- secure disposal of paper and electronic records;
- clear handover arrangements when councillors, employees or contractors leave their role.

15.3 Personal data should not be stored on personal devices unless the Council has authorised this and appropriate security measures are in place.

15.4 Council emails and documents should be sent using Council-approved systems wherever possible. Personal email accounts should not be used for Council business unless there is no reasonable alternative and the information is not sensitive.

16. Records retention, archiving and disposal

16.1 Personal data must be kept only for as long as necessary for the purpose for which it was collected, unless a longer period is required for legal, audit, historical, archival or public interest reasons.

16.2 The Council will maintain a records retention schedule setting out retention periods for key categories of records, including minutes, agendas, finance records, employment records, contracts, complaints, correspondence, insurance, asset records and event records.

16.3 Records selected for permanent preservation, such as signed minutes and historically significant council records, may be retained for archiving in the public interest where lawful safeguards are applied.

16.4 Paper records containing personal data must be shredded or disposed of securely. Electronic records must be deleted securely from live systems and, where practical, from backups at the end of their retention period.

17. Sharing personal data and using processors

17.1 The Council will share personal data only where there is a lawful basis and it is necessary and proportionate.

17.2 Personal data may be shared with auditors, payroll providers, HMRC, pension providers, insurers, banks, IT and website providers, legal advisers, contractors, the Vale of Glamorgan Council, Welsh Government, the Public Services Ombudsman for Wales, the Information Commissioner's Office, police or other regulatory bodies where lawful and necessary.

17.3 Where the Council uses a processor, there must be a written contract or agreement requiring the processor to protect personal data, act only on Council instructions, maintain confidentiality, apply appropriate security, assist with rights requests and breaches, and delete or return data at the end of the service.

17.4 International transfers of personal data outside the UK must not take place unless appropriate safeguards or lawful transfer mechanisms are in place.

18. Electronic communications and direct marketing

18.1 The Council will comply with PECR where it sends electronic communications that amount to direct marketing.

18.2 Routine Council communications, statutory notices, meeting papers, service administration and responses to enquiries are not normally direct marketing, but they must still comply with UK GDPR and this policy.

18.3 Consent or another lawful route may be needed for optional newsletters, event publicity mailing lists, non-statutory promotional messages or similar communications. Individuals must be able to unsubscribe or withdraw consent where consent is relied upon.

18.4 The Council will not add individuals to optional mailing lists simply because they have contacted the Council for another reason.

19. Councillors and personal data

19.1 Councillors must handle personal data carefully and only use Council-provided personal data for authorised Council business.

19.2 Councillors should not forward Council personal data to private individuals, unauthorised organisations or personal networks unless there is a lawful basis and Council authority to do so.

19.3 Where a councillor receives personal data as part of their role on the Council, it should be stored securely, retained only while needed and deleted or returned when no longer required.

19.4 Where a councillor acts independently, for example in party-political, election, campaign or personal casework activity outside Council business, they may have their own data protection responsibilities and should not assume that the Council is the controller for that activity.

19.5 Councillors must report any suspected breach involving Council personal data to the Proper Officer immediately.

20. Training, monitoring and review

20.1 Councillors and staff should receive appropriate data protection awareness information when they take office or start work, and refresher guidance when policies, systems or legal requirements change.

20.2 The Council will review this policy at least every two years, or sooner if there is a significant change in legislation, ICO guidance, Council services, technology, staffing or data protection risk.

20.3 The Proper Officer will bring significant data protection risks, breaches, repeated issues or policy changes to Council or the appropriate committee, while protecting confidential personal data.

21. Related policies and records

21.1 This policy should be read alongside the following Council documents, where adopted:

- Privacy notices;
- Records Retention / Document Retention Policy;
- Freedom of Information Publication Scheme;
- Complaints Policy;
- Disciplinary and Grievance Policy;
- Equality and Diversity Policy;
- Welsh Language Policy;
- Social Media and Digital Communications Policy;
- Meeting Recording Policy or privacy notice, where audio recording is used for accuracy of minutes;
- IT, cyber-security or acceptable use procedures;
- Data processing contracts and supplier due diligence records;
- Data breach log;
- Subject access and data rights request log;
- Data protection complaints log.

Appendix 1 - Quick checklist for the Proper Officer

- Keep the Council's privacy notices up to date.
- Maintain a record of processing activities appropriate to the Council's size and risk.
- Maintain a records retention schedule and arrange secure disposal when required.
- Log all subject access requests and other data rights requests.
- Log all data protection complaints and acknowledge them within 30 days.
- Log all suspected and confirmed personal data breaches.
- Assess notifiable breaches quickly enough to meet the 72-hour reporting window where required.
- Check documents before website publication to avoid accidental disclosure of personal data.
- Use data processing contracts for payroll, IT, website, cloud, accounting and other processors.
- Ensure councillors and staff receive basic data protection awareness information.
- Review consent arrangements and avoid using consent where another lawful basis is more appropriate.
- Keep evidence of decisions, lawful bases and data-sharing decisions where appropriate.

Appendix 2 - Staff and councillor data protection acknowledgement

This acknowledgement replaces the previous general "GDPR consent form". It is not a consent form for ordinary Council business. It confirms that councillors and staff understand their responsibility to handle personal data lawfully and securely.

Name: _____

Role: _____

I confirm that I have received or been given access to the Council's UK GDPR and Data Protection Policy and agree to follow it when handling personal data for Council business.

I understand that I must:

- use personal data only for authorised Council purposes;
- keep personal data secure and confidential;
- avoid unnecessary copying, forwarding, downloading or printing of personal data;
- not disclose personal data unless authorised and lawful;
- report suspected data breaches or data protection concerns to the Proper Officer immediately;
- return or securely delete Council personal data when I leave office, employment or my authorised role.

Signed: _____

Date: _____

Optional communication preferences

The Council may need to contact councillors and staff for Council administration using contact details it holds under an appropriate lawful basis. The preferences below help the Council use practical contact methods where possible. They do not prevent the Council from communicating where it has a lawful basis or legal obligation to do so.

Contact method	Preferred?	Details / notes
Council email	Yes / No	
Personal email if authorised	Yes / No	
Post	Yes / No	
Mobile phone	Yes / No	

Text message / WhatsApp if authorised	Yes / No	
Home telephone	Yes / No	

Reference sources used for this update

This policy has been updated by reference to the current UK data protection framework, including the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, ICO guidance and PECR. The Council should check current ICO guidance when reviewing or applying this policy.

- Information Commissioner's Office - UK GDPR guidance and resources
- Information Commissioner's Office - Data protection principles
- Information Commissioner's Office - Subject access requests
- Information Commissioner's Office - Data protection complaints guidance
- Information Commissioner's Office - Personal data breach reporting guidance
- legislation.gov.uk - Data Protection Act 2018
- legislation.gov.uk - Data (Use and Access) Act 2025
- legislation.gov.uk - Privacy and Electronic Communications Regulations 2003