BARLASTON PARISH COUNCIL

APPROPRIATE POLICY DOCUMENT

GDPR10

APPROPRIATE POLICY DOCUMENT

Revision History

This document was originally written by:

Name	**Position**	**Date**
Vivien O'Dunne	Clerk	February 2026

This document was reviewed by:

The Parish Council	10 March 2026

This document version was adopted by:

The Parish Council at their meeting on	10 March 2026

Document Review schedule:

Next Mandatory Review by	March 2027

Version	**Issue Date**	**Document ID**	**Reason for Change**	**Section changed**
1	10 March 2026	GDPR10	Revised Policy – Assertion 10 2025/26	Major Review

Appropriate Policy Document template

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document should demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it should outline your retention policies with respect to this data. (See Schedule 1 Part 4).

If you process SC or CO data for a number of different purposes you do not need a separate policy document for each condition or processing activity – one document can cover them all. You may reference policies and procedures which are relevant to all the identified processing. Whilst you may explain your compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, you should provide the data subject with sufficient information to understand how you are processing their SC or CO data and how long you will retain it for.

However if you rely on one of these conditions, your general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;
(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

The APD therefore complements your general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge. See Schedule 1 Part 4 paragraph 40.

You should read this document alongside our Guide to the GDPR.

Note your APD does not have to be structured in accordance with this document. This template is intended as a guideline only.

Description of data processed

Give a brief description of each category of SC/CO data processed. You may wish to refer to your Article 30 record of processing for that particular data:

The Council processes the following categories of SC/CO personal data (see Data Map / Article 30 Record of Processing Activities):

- Staff (Clerk/RFO): Payroll, pension, employment records, leave, sickness, HR files (SC)
- Residents/Public Correspondence: Sensitive complaints or enquiry information (SC if health or other protected data disclosed)
- Elected Members: Register of interests, roles, contact details (public task/legal obligation; limited SC if disclosed)
- CCTV: Video footage for crime prevention and safety (SC/legitimate interest)
- Cloud/IT Storage: SC data stored securely (Dropbox, payroll, HR, correspondence)
- Historic/Legacy Records: Limited SC data in archived correspondence or employment files

Schedule 1 condition for processing

Give the name and paragraph number of your relevant Schedule 1 condition(s) for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

The Council relies on the following conditions under Schedule 1 Part 2 of DPA 2018:

- Employment, social security, and social protection law (staff HR, payroll, pensions)
- Substantial public interest (residents' complaints with sensitive data)
- Crime prevention / legal obligation (CCTV, public safety)

This APD references related policies, the Data Map, CCTV DPIA, and Risk Register to demonstrate compliance.

Procedures for ensuring compliance with the principles

You need to explain, in brief and with reference to the conditions relied upon, how your procedures ensure your compliance with the principles below.

This helps you meet your accountability obligations. You have a responsibility to demonstrate that your policies and procedures ensure your compliance with the wider requirements of the GDPR and in particular the principles. The sensitivity of SC and CO data means the technical and organisational measures you have in place to protect such data are crucially important.

The questions listed in each box are intended to help you describe how you satisfy each principle generally, and are based on the checklist for each principle provided in the Guide to the GDPR. They are not exhaustive and are only intended to act as a guideline.

In explaining your compliance with the principles you should consider the specifics of your processing with respect to the SC and CO data you have identified above.

You may also wish to answer other questions which are included in our Guide to the GDPR checklists (see links in each section below).

There is also no requirement to reproduce information which is recorded elsewhere – questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.

Accountability principle
i. Do we maintain appropriate documentation of our processing activities? Yes. Barlaston Parish Council maintains an Article 30 Record of Processing Activities (Data Map) covering all personal data processed, including categories of data, lawful bases, retention periods, recipients, security measures, and any special category or high-risk processing. ii. Do we have appropriate data protection policies? Yes. The Council has an Appropriate Policy Document (APD) and supporting policies, including: Data Handling Policy, Data Security Policy, CCTV Policy, Rights Requests Policy, and Privacy Notices. These are reviewed annually or sooner if processing activities change materially. iii. Do we carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' interests? Yes. Mini DPIAs are carried out for higher-risk processing such as CCTV, cloud storage of sensitive data, and special category data. Outcomes, residual risks, and mitigations are documented, and reviews are conducted periodically.
Principle (a): lawfulness, fairness and transparency
i. Have we identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data? Yes. All personal data is processed on a lawful basis under GDPR Article 6 (public task, legal obligation, or contract). Special category data (e.g., payroll, pensions, health data) is processed under Schedule 1 conditions of the Data Protection Act 2018, including employment, social security, and substantial public interest conditions. Each processing activity is documented in the Data Map / Article 30 Record. ii. Do we make appropriate privacy information available with respect to the SC/CO data? Yes. The Council publishes a Privacy Notice for the public and provides staff and councillors with guidance on handling personal data. Privacy

information covers purposes, lawful basis, retention periods, rights, recipients, and data subject access.

iii. Are we open and honest when we collect the SC/CO data and do we ensure we do not deceive or mislead people about its use?

Yes. The Council ensures transparency at the point of collection by providing privacy notices on forms, emails, website, CCTV signage, and surveys. Individuals are informed why their data is collected, how it will be used, who it may be shared with, and how long it will be retained.

Principle (b): purpose limitation

i. Have we clearly identified our purpose(s) for processing the SC/CO data?
Yes. Each category of SC/CO data is processed only for clearly defined statutory, financial, employment, or administrative purposes. Examples include payroll and pension management, staff employment records, CCTV for crime prevention, and resident correspondence for enquiries or complaints. All purposes are documented in the Data Map / Article 30 Record.

ii. Have we included appropriate details of these purposes in our privacy information for individuals?
Yes. The Council's Privacy Notice and point-of-collection information clearly describe why SC/CO data is collected, what it will be used for, who it may be shared with, and the lawful basis for processing. This ensures individuals understand the purposes of processing.

iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), do we check that this is compatible with our original purpose or get specific consent for the new purpose?

Yes. Any new processing activity is assessed for compatibility with the original purpose. Where the new purpose is not compatible or statutory/legal, the Council will seek explicit consent from the individual before processing.

Principle (c): data minimisation

i. Are we satisfied that we only collect SC/CO personal data we actually need for our specified purposes?
Yes. The Council collects only the SC/CO data necessary to carry out statutory, employment, financial, or administrative functions. For example, payroll records include only the details required for salary calculation and pension contributions; CCTV footage is recorded solely for crime prevention and safety monitoring.

ii.	Are we satisfied that we have sufficient SC/CO data to properly fulfil those purposes? Yes. The Council ensures that the data collected is sufficient to meet legal and operational requirements without collecting unnecessary information. No extra personal data is held beyond what is required for the defined purpose.
iii.	Do we periodically review this particular SC/CO data, and delete anything we don't need? Yes. The Council follows a retention schedule and routinely reviews records. SC/CO data is deleted or securely destroyed when no longer required, unless retention is required by law or for historical/public interest purposes. Mini DPIAs and the Data Map support ongoing review.
Principle (d): accuracy	
i.	Do we have appropriate processes in place to check the accuracy of the SC/CO data we collect, and do we record the source of that data? Yes. The Council collects most SC/CO data directly from the individual concerned (e.g., staff employment and payroll information), ensuring accuracy at the point of collection. Where data is obtained from third parties (e.g., pension providers or statutory bodies), the source is recorded within the relevant file or system. Information is checked for completeness and relevance before being stored.
ii.	Do we have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and do we update it as necessary? Yes. Employment and payroll records are reviewed and updated as part of routine administrative processes. Individuals are encouraged to notify the Council of any changes to their details. Records are updated promptly where necessary to ensure they remain accurate and fit for purpose.
iii.	Do we have a policy or set of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification? Yes. The Council's Data Handling and Rights Requests procedures set out how requests for rectification are managed. Where inaccuracies are identified, corrections are made promptly and, where appropriate, a record of the amendment is retained. Individuals are informed of the outcome of their request within the statutory timeframe.
Principle (e): storage limitation	
i.	Do we carefully consider how long we keep the SC/CO data and can we justify this amount of time? Yes. The Council applies a documented retention schedule to all SC/CO data. Retention periods are based on statutory requirements, audit obligations, employment law, and operational necessity. For example, employment and payroll records are retained for six years after employment ends; finance records are retained for six years for audit

purposes; CCTV footage is retained for 31 days. Each retention period can be justified by legal or administrative need.

ii. Do we regularly review our information and erase or anonymise this SC/CO data when we no longer need it?
Yes. Records are reviewed periodically in line with the retention schedule. SC/CO data is securely destroyed (paper records shredded; digital data permanently deleted) when it is no longer required. Cloud-stored and email data are also reviewed and deleted in accordance with operational need and retention rules.

iii. Have we clearly identified any SC/CO data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes?
Yes. Where records are retained for statutory, audit, or historical purposes (e.g., certain legacy council records), this is documented in the Data Map. Only relevant information is retained, and access is restricted. Special category data is not retained for research or statistical purposes unless required by law.

Principle (f): integrity and confidentiality (security)

i. Have we analysed the risks presented by our processing and used this to assess the appropriate level of security we need for this data?
Yes. The Council has assessed risks associated with processing SC/CO data through its Data Map (Article 30 record), Risk Register, and Mini Data Protection Impact Assessments (DPIAs) where appropriate (e.g., CCTV and cloud storage). Risks such as unauthorised access, accidental disclosure, loss, or misuse have been identified and proportionate technical and organisational measures have been implemented to mitigate them. Residual risks are assessed as low to medium and reviewed periodically.

ii. Do we have an information security policy (or equivalent) regarding this SC/CO data and do we take steps to make sure the policy is implemented? Is it regularly reviewed?
Yes. The Council has a Data Security Policy and Data Handling Policy, supported by this Appropriate Policy Document. These outline secure storage, access controls, breach reporting procedures, and staff responsibilities. Policies are reviewed annually or sooner if processing activities change. Councillors and staff are made aware of their responsibilities through guidance and training.

iii. Have we put other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing?
Yes. The Council applies appropriate safeguards including:

- Password-protected systems and secure devices
- Two-factor authentication where available
- Restricted access to authorised personnel only
- Secure cloud storage with contractual safeguards in place
- Locked storage for paper records
- Secure destruction of records when retention periods expire
- Breach reporting and incident logging procedures

These measures ensure that SC/CO data is protected against unauthorised or unlawful processing, accidental loss, destruction, or damage.

Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of SC/CO data (this could include a link to your retention policy if you have one). You need to explicitly indicate how long you are likely to retain each specific category of SC/CO data.

Barlaston Parish Council retains Special Category (SC) data only for as long as necessary to fulfil statutory, employment, financial, or administrative purposes. Retention periods are documented in the Council's Retention Schedule and Data Map (Article 30 Record).
The following retention periods apply:
1. Employment and Payroll Records (Special Category data – health, payroll, pension information)
Retention period: 6 years after employment ends.
Erasure method: Secure destruction of paper records (shredding) and permanent deletion of digital records from local and cloud systems.
2. Pension Records (Special Category data)
Retention period: 6 years after employment ends (or longer where required by pension regulations).
Erasure method: Secure deletion and destruction in line with statutory requirements.
3. Sickness and HR Records (Special Category data)
Retention period: Duration of employment plus 6 years.
Erasure method: Secure shredding of paper files and permanent digital deletion.
4. CCTV Footage (may contain Special Category data)
Retention period: 31 days, unless required for investigation or legal proceedings.
Erasure method: Automatic overwriting after 31 days; manual secure deletion where required.
5. Residents' Complaints or Correspondence containing Special Category data
Retention period: Deleted once the matter is resolved and no further action is required, unless required for legal purposes.
Erasure method: Secure deletion of electronic records and shredding of paper copies.
6. Finance and Supplier Records (may incidentally include SC data)
Retention period: 6 years for audit and accounting purposes.
Erasure method: Secure destruction in accordance with financial retention requirements.
7. Historic or Archived Records containing limited SC data
Retention period: Retained only where required for statutory, audit, or historical purposes.

Erasure method: Phased review and secure destruction where continued retention is no longer justified.
The Council reviews retained records periodically to ensure data is not kept longer than necessary. Where retention periods expire, records are securely destroyed or anonymised. Any deviation from the retention schedule is documented and justified.

APD review date

The APD will always be reviewed immediately if significant changes to processing occur, in addition to the annual review cycle.

Chairman

Date: 10 March 2026