CAPEL PARISH COUNCIL

Information Governance Policy

Data protection, freedom of information, security and record keeping in one place

Status	Final	**Policy owner**	Parish Clerk
Adopted	November 2026	**Minute reference**	Item 18, 16/11/2026
Last reviewed	November 2026	**Next review**	November 2027
Review cycle	Annual	**Applies to**	Council, committees, staff and members

1. Purpose and legal framework

The Council holds personal and public information and must handle it lawfully. This single policy covers: data protection; requests for information and for personal data; data breaches; data protection complaints; security; and retention. It brings together what would otherwise be separate data protection, FOI/subject access, breach and retention policies. The main laws are the UK GDPR, the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025), the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).

2. Roles

- **The Council** is the data controller and is responsible for compliance. It is registered with, and pays the data protection fee to, the Information Commissioner's Office (ICO).
- **Data Protection Officer (DPO):** parish councils are public authorities and must appoint a DPO. The DPO is to be appointed and is independent and not the Clerk or a councillor.
- **The Clerk** is the first point of contact, keeps the information asset register and retention schedule, and handles requests and breaches.
- **Councillors and staff** must follow this policy, use Council email accounts, and report problems at once.

3. Data protection principles

We process personal data lawfully, fairly and transparently; only for specified purposes; in an adequate, relevant and limited way; accurately; kept no longer than necessary; and securely. We tell people how we use their data in our Privacy Notices, rely on a lawful basis (usually public task, legal obligation or contract), and complete a data protection impact assessment before any high-risk new use (for example CCTV).

4. Security

- Use Council-provided accounts and approved storage; no personal email for Council business.
- Strong unique passwords and multi-factor authentication where available. Do not share passwords.
- Lock or encrypt devices, keep software updated, use blind copy where recipients should not see each other, and check attachments.
- Do not put personal or confidential Council information into unapproved online tools, including public artificial intelligence services.
- Paper records are locked away. Back-ups are held separately and tested.

- When a councillor or employee leaves, access is removed and records are returned.

5. Requests for information

Freedom of Information and Environmental Information

- Requests must be in writing (email is fine), give a name and address for reply, and describe the information. The Clerk logs every request.
- We reply within **20 working days**. Information that is already published under the Publication Scheme will be pointed to.
- We may refuse information that is exempt (for example personal data, commercially sensitive or legally privileged information) or where the cost limit is exceeded, giving reasons and the right to ask for an internal review and to complain to the ICO.
- We do not charge for information on the website; we may charge only for actual printing, copying and postage, and will say so in advance.

Subject access and other personal data rights

- Individuals can ask for a copy of their personal data and to correct, erase, restrict or object to its use, where the law allows.
- We reply within **one month**, extendable by up to two months for complex requests. We do reasonable and proportionate searches and may ask for proof of identity or for clarification (which pauses the clock).
- Councillors must pass any request received to the Clerk the same day.

6. Personal data breaches

A breach is any loss, theft, wrongful disclosure or alteration of personal data (for example a misdirected email or lost laptop).

1. Report it to the Clerk immediately (to the Chair if the Clerk is involved). Do not try to hide or fix it alone.

2. The Clerk records it in the breach log, contains it and assesses the risk, with the DPO.

3. If there is a risk to people's rights, we report it to the **ICO within 72 hours** of becoming aware, and tell the people affected without undue delay if the risk is high.

4. The Council reviews what happened and what to change.

7. Data protection complaints

Since 19 June 2026 controllers must provide a way to complain about how their data is handled. Anyone may complain to the Clerk (clerk@capel-pc.gov.uk) or the DPO, in any form. We acknowledge within **30 days**, investigate, and tell the person the outcome. They may also complain to the ICO. This route is separate from the general Complaints Procedure.

8. Retention and disposal

Records are kept for the periods in the Retention Schedule below, then securely destroyed or deleted (confidential waste for paper; secure deletion for electronic). Records that must be kept permanently, or that the public may inspect, are kept in an organised filing structure. Any decision to keep records beyond the periods needs a reason.

Retention Schedule

Periods are minimum guides based on the NALC/SLCC Practitioners' Guide and common law-firm and ICO practice. The Council's DPO or auditor should confirm the final schedule. "Permanent" means keep for the life of the Council and consider archiving.

Record	Keep for	Reason
Minutes, agendas and signed minute books	Permanent	Statutory (Local Government Act 1972, Sch 12); history
Standing Orders, Financial Regulations, policies (current and superseded)	Permanent	Governance record
Statutory registers (interests, gifts, assets)	Permanent / until superseded	Statutory and audit
Title deeds, leases, land records, burial registers and cemetery plans	Permanent	Legal title; Local Authorities' Cemeteries Order 1977
Annual Governance and Accountability Returns, audit reports	Permanent (or at least 6 years)	Audit; transparency
Cash books, bank statements, ledgers, budgets, precept papers	6 years after the year end	Limitation Act 1980; HMRC
Paid invoices, receipts, orders, contracts (simple)	6 years after the year end	Audit; Limitation Act
Contracts under seal / deeds	12 years after the contract ends	Limitation Act 1980
VAT records	6 years	VAT Act 1994
Payroll, pension and PAYE records	6 years after the year end	HMRC; pensions
Employee personal files	6 years after employment ends	Limitation Act; references
Recruitment: unsuccessful applicants	6 months after the decision	Equality Act claims
Disclosure and Barring Service check results	Record that a check was done; do not keep the certificate beyond 6 months	DBS code of practice
Sickness and absence records	6 years after the year end (SSP: 3 years minimum)	SSP rules; employment law
Accident and incident records, RIDDOR	At least 3 years; for children until age 21	RIDDOR 2013; limitation
Risk assessments, inspection records (play areas, buildings)	Life of the equipment plus 6 years	Health and safety; insurance claims
Insurance policies and certificates	Permanent for liability policies; claims 6 years after closure	Latent claims
Complaints files	6 years after closure	Limitation Act
Safeguarding records	Until the child is 25 / adult 6 years after case closure, or as advised by the safeguarding authority	Safeguarding guidance
Allotment tenancies, hall hire bookings	6 years after the tenancy or booking ends	Contract claims
Planning consultation responses	Until the application is decided and any appeal ends, then 2 years	Operational
General correspondence and enquiries	2 years	Operational
Subject access requests, FOI requests and breach logs	3 years after closure	ICO accountability
CCTV recordings (if used)	31 days unless needed for an incident	ICO guidance
Photographs and consent forms	While used, plus 1 year; consent forms until the use ends	Consent
Social media and website content	Archive important posts as records; delete others after 1 year	Records management