CHIGWELL PARISH COUNCIL

INFORMATION & DATA PROTECTION POLICY

Draft for review and adoption at the Parish Council meeting on 21 May 2026

Supersedes: Information & Data Protection Policy adopted 13 May 2025

Policy owner	Clerk / Proper Officer
Responsible committee	Full Council, with oversight by the Finance and Governance Committee where delegated
Data protection contact	Clerk / Proper Officer through the Council's published contact details
Status	Draft for Council review and adoption
Adoption date	21 May 2026, subject to Council resolution
Next scheduled review	May 2027, or earlier if legislation, ICO guidance, Council systems or Council operations change materially
Minute reference	

Adoption confirmation

Chair signature	
Date	
Minute number	

1. Purpose

Chigwell Parish Council (the Council) processes information in order to carry out its statutory functions, deliver services, manage employees, support councillors and volunteers, communicate with residents, maintain assets and facilities, meet its legal obligations and promote transparent local governance.

This policy sets out how the Council will manage information, protect personal data and confidential information, and make appropriate information available to the public. It applies to all councillors, employees, workers, volunteers, contractors, processors and any other person handling information for, or on behalf of, the Council.

This policy should be read alongside the Council's Publication Scheme, Data Retention Policy, Email Usage Policy, Email, Communications and Media Policy, IT Policy, CCTV Privacy Policy, privacy notices, Standing Orders and Financial Regulations.

2. Scope of information covered

The Council handles a range of information, including:

- Public information that the Council makes available through agendas, minutes, the website, noticeboards, consultations, reports, transparency publications and public communications.
- Official Council information that may not yet be published, including draft reports, working papers, project information, legal advice, committee papers and operational records.
- Confidential and commercially sensitive information about the Council, contractors, suppliers, partner organisations, negotiations, tenders, land, leases, staff matters and legal matters.
- Personal data relating to current, former and prospective employees, councillors, volunteers, contractors and applicants.
- Personal data relating to residents, service users, complainants, correspondents, cemetery users, allotment holders, hirers, grant applicants, consultation respondents, suppliers and members of the public who contact the Council.
- Special category data and other sensitive information where necessary, for example equality monitoring information, health information, safeguarding information, disability access information, criminal conviction or Disclosure and Barring Service information, or information about children and vulnerable people.

3. Legal and regulatory framework

The Council will comply with all applicable information rights and data protection law. The principal framework includes, where relevant:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025 and commencement regulations, including changes to subject access, complaints handling, recognised legitimate interests, international transfers and the Information Commissioner's functions.
- Freedom of Information Act 2000.
- Environmental Information Regulations 2004.
- Privacy and Electronic Communications Regulations 2003.
- Local Government Act 1972, Public Bodies (Admission to Meetings) Act 1960 and the Openness of Local Government Bodies Regulations 2014.
- Local Government Transparency Code 2015, where applicable to the Council by income or expenditure threshold or as a matter of good practice.
- Common law duties of confidentiality, contractual confidentiality obligations and employment obligations.

- Disclosure and Barring Service requirements and its Code of Practice where DBS checks are undertaken.

The Council will keep this policy under review in light of legislation, ICO guidance, good practice for local councils and experience of handling information requests, complaints, incidents and service delivery.

4. Data protection principles

The Council will process personal data in accordance with the data protection principles. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used in a way that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- processed securely, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- handled in a way that enables the Council to demonstrate accountability.

5. Key definitions

Term	Meaning
Personal data	Any information relating to an identified or identifiable living individual. This includes names, addresses, telephone numbers, email addresses, photographs, identification numbers, online identifiers, location data, opinions about a person and information which can identify a person when combined with other information.
Special category data	More sensitive personal data requiring additional protection. This includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for identification, health data, sex life and sexual orientation.
Criminal offence data	Personal data relating to criminal convictions, offences, allegations, proceedings or related security measures.
Data subject	The individual whom personal data relates to.
Controller	The person or organisation that determines the purposes and means of processing personal data. The Council is normally the controller for personal data it collects and uses for Council purposes.
Processor	A person or organisation that processes personal data on behalf of the Council under the Council's instructions, such as an IT provider, payroll provider, website provider or other contractor.
Processing	Any operation performed on personal data, including collection, recording, storage, alteration, retrieval, consultation, use, disclosure, sharing, restriction, erasure or destruction.

Official information	Recorded information held by, or on behalf of, the Council for Council purposes, regardless of the account, device, platform or location where it is stored.

6. Roles and responsibilities

6.1 Council

The Council is responsible corporately for compliance with data protection and information rights legislation. It will ensure that appropriate policies, procedures, resources, training and records are in place.

6.2 Clerk / Proper Officer

The Clerk / Proper Officer is responsible for the day-to-day management of information governance, supported by staff and councillors as required. This includes receiving and coordinating subject access requests, freedom of information requests, environmental information requests, complaints, personal data breach reports and liaison with the ICO.

The Clerk / Proper Officer is the Council's nominated Data Protection Lead unless the Council separately appoints a Data Protection Officer or external adviser. If the Council appoints a Data Protection Officer, the Council will ensure that the role is independent, appropriately resourced and free from conflicts of interest.

6.3 Councillors

Councillors must handle Council information responsibly, lawfully and securely. Councillors must only access or use personal data where it is necessary for Council purposes, for their Council role, or for legitimate ward or casework activity consistent with applicable law and Council policies.

Councillors must distinguish between Council business, ward casework, party political activity, election campaigning, private business and personal matters. Council resources, Council email addresses and Council-held personal data must not be used for party political, electoral, personal or commercial purposes.

6.4 Employees, workers and volunteers

Employees, workers and volunteers must comply with this policy, their contracts or role descriptions, Council procedures and instructions from the Clerk / Proper Officer. They must keep personal data confidential and report incidents or concerns immediately.

6.5 Contractors, suppliers and processors

Contractors, suppliers and processors must comply with written contract terms and data processing obligations. The Council will ensure that processors provide sufficient guarantees about security and only process personal data on documented Council instructions.

7. Lawful basis for processing

The Council will identify and record an appropriate lawful basis before processing personal data. Depending on the activity, this may include:

- consent, where the individual has given clear consent and can withdraw it;
- contract, where processing is necessary for a contract with the individual or to take steps before entering into a contract;
- legal obligation, where processing is necessary to comply with law;

- vital interests, where processing is necessary to protect someone's life;
- public task, where processing is necessary for the Council to perform its public functions or exercise official authority;
- legitimate interests, where available and appropriate, and only where the Council has considered the interests, rights and freedoms of individuals.

The Council will not rely on consent where another lawful basis is more appropriate, particularly where there is an imbalance of power or the Council has a statutory duty to act.

Special category data and criminal offence data will only be processed where a lawful basis and an additional legal condition apply. The Council will apply appropriate safeguards, restrict access and retain such information only for as long as necessary.

8. Transparency and privacy notices

The Council will be open with individuals about how their personal data is used. Privacy notices will explain what information is collected, why it is used, the lawful basis, who it may be shared with, how long it is kept, individual rights and how to contact the Council.

Privacy information will be provided at appropriate points, including when people use Council services, apply for employment, make complaints, respond to consultations, hire facilities, apply for grants, communicate with councillors or otherwise provide personal data.

9. Information security

The Council will apply appropriate technical and organisational measures to protect information. These may include access controls, password protection, multi-factor authentication where available, secure backup, encryption where appropriate, audit trails, locked storage, secure disposal, staff instructions and contractual safeguards.

Councillors, staff and volunteers must:

- keep passwords confidential and not share user accounts;
- lock devices and protect paper records from unauthorised viewing;
- use secure methods to send personal or confidential information;
- check recipients carefully before sending emails or documents;
- use blind copy (bcc) when emailing groups of individuals unless disclosure of addresses is justified and approved;
- avoid unnecessary duplication, downloading or printing of personal data;
- store Council records only in approved Council systems, folders or repositories;
- not use personal cloud storage, personal messaging apps or private storage for Council records unless expressly authorised by the Clerk / Proper Officer in exceptional circumstances;
- return or securely delete Council information when their role ends or when instructed; and
- report suspected loss, misuse, unauthorised disclosure, cyber incident or other data breach immediately.

10. Mandatory use of Council email addresses

Council email requirement: Councillors and staff must use their Council-provided @chigwellparishcouncil.gov.uk email address for all Council-related matters. Personal email accounts must not be used for Council business except in a genuine emergency or where expressly authorised by the Clerk / Proper Officer. If personal email, personal devices or non-corporate channels are used for Council business, the information remains subject to the Council's data protection, confidentiality, retention, subject access, freedom of information and environmental information obligations.

All councillors and staff must conduct Council-related business using their Council-provided @chigwellparishcouncil.gov.uk email address and approved Council systems. This includes communications with residents, other councillors, staff, contractors, public bodies, partner organisations, press contacts and suppliers about Council business.

Council email addresses must not be used for election activity, private business, personal matters or in communications that could be mistaken for an official Council position or communication when no such authority exists.

10.1 Prohibited or restricted practices

Councillors and staff must not:

- routinely send, receive, forward, copy or blind copy Council business to or from a personal email account
- make representations or statements on behalf of the Council or as a member of staff or councillor from a personal account
- set automatic forwarding from a Council email account to a personal account
- store Council documents or personal data in personal email folders, personal cloud accounts or private messaging platforms
- use a shared family, business or political-party email account for any Council business or communication whatsoever
- continue Council correspondence from a personal account after receiving a Council email account
- delete Council-related correspondence from personal or Council accounts to avoid retention, disclosure, audit or request obligations
- remove Council information from approved systems without a legitimate Council purpose.

10.3 Exceptional use of personal email

Personal email may only be used in exceptional circumstances, for example where a Council system is unavailable and urgent action is required to protect safety, property, Council interests or statutory deadlines. Where this happens, the councillor or staff member must:

- use the minimum information necessary;
- avoid sending special category, criminal offence, financial, confidential or sensitive information unless there is no safe alternative and the matter is urgent;
- copy or forward the full record to their Council email address and/or the Clerk / Proper Officer as soon as practicable;
- tell the Clerk / Proper Officer that personal email has been used and why;
- securely delete the Council information from the personal account, including sent items and deleted items, once it has been captured in Council systems unless instructed otherwise; and
- cooperate with any later search, retention, audit or access request.

10.4 Personal email remains disclosable and searchable

Where Council-related information is held in a personal email account, on a personal device, in a personal messaging account or in any other non-corporate channel, it may be held on behalf of the Council. It can therefore fall within the scope of subject access requests, freedom of information requests, environmental information requests, court proceedings, regulatory investigations, audit requirements, complaints and internal reviews.

Councillors and staff must, when asked by the Clerk / Proper Officer or an authorised officer, promptly search personal accounts, devices or non-corporate channels for Council-related information that may be relevant to a lawful request, complaint, investigation, audit, disclosure exercise or retention requirement. They must provide the relevant records to the Council and must not alter, conceal or destroy them.

Failure to use Council email addresses or to cooperate with searches may expose the Council and the individual to legal, regulatory, reputational and disciplinary consequences.

11. Record keeping and retention

The Council will maintain records sufficient to demonstrate decisions, actions, legal compliance, financial accountability, service delivery and transparency. Records must be stored in approved Council systems and retained in line with the Council's Data Retention Policy and any applicable legal, audit or insurance requirements.

Councillors and staff must ensure that Council-related records are available to the Council and not solely held in individual mailboxes, personal folders or devices. Where a communication forms part of a decision, case, complaint, contract, project, grant, personnel matter or service record, it must be filed or captured in the appropriate Council record system.

Personal data must not be kept longer than necessary. Secure disposal methods must be used for paper and electronic records, including confidential waste, secure deletion and supplier disposal arrangements where appropriate.

12. Data sharing

The Council will share personal data only where there is a lawful basis, a legitimate purpose and appropriate safeguards. Sharing may occur with other local authorities, public bodies, regulators, law enforcement agencies, payroll providers, pension providers, insurers, professional advisers, auditors, IT suppliers, contractors, partner organisations and others where necessary.

Before sharing personal data, the Council will consider:

- why the information is being shared and whether sharing is necessary and proportionate;
- the lawful basis and any special category or criminal offence data condition;
- whether the recipient is a controller, joint controller or processor;
- whether a written agreement, data sharing agreement or data processing contract is needed;
- what information should be shared and whether it can be minimised or anonymised;
- security measures for transfer and storage;
- retention and deletion arrangements; and
- whether individuals need additional privacy information.

13. International transfers

Personal data must not be transferred outside the United Kingdom unless the Council has assessed the transfer and appropriate safeguards are in place. This may include UK adequacy regulations, an appropriate international data transfer agreement, UK addendum, binding corporate rules, transfer risk assessment, or another lawful transfer mechanism.

Councillors and staff must not use overseas, personal or unapproved systems to store or process Council personal data unless approved by the Clerk / Proper Officer following a suitable assessment.

14. Data protection by design and impact assessments

The Council will consider privacy and information security at the start of new projects, services, procurement, systems, consultations and processing activities. Where processing is likely to result in a high risk to individuals, the Council will complete a Data Protection Impact Assessment before processing begins.

Examples of activities that may require additional assessment include new CCTV or surveillance arrangements, new online forms or systems, large-scale data sharing, processing children's data, processing special category information, new cemetery or facility management systems, or use of automated tools or artificial intelligence.

15. Children and vulnerable people

The Council will take particular care when processing information about children and vulnerable people. Where consent is relied upon for a child, the Council will consider whether parental or guardian consent is required and whether the child has sufficient understanding to consent themselves.

Information about children or vulnerable people will be collected only where necessary, handled confidentially, shared only where lawful and proportionate, and protected through suitable safeguards. Safeguarding concerns must be escalated in accordance with Council procedures and relevant law.

16. Rights of individuals

Individuals have rights under data protection law, subject to conditions and exemptions. These rights include:

- the right to be informed about how their data is used;
- the right of access to their personal data (subject access);
- the right to rectification of inaccurate data;
- the right to erasure in certain circumstances;
- the right to restrict processing in certain circumstances;
- the right to data portability in limited circumstances;
- the right to object in certain circumstances; and
- rights relating to automated decision-making and profiling.

The Council does not make solely automated decisions about individuals which produce legal or similarly significant effects, unless a separate approved process and privacy notice states otherwise.

Requests may be made verbally or in writing. Staff and councillors must forward any request that may relate to personal data rights to the Clerk / Proper Officer immediately, even if the request does not use legal terminology.

16.1 Subject access requests

The Council will respond to subject access requests without undue delay and within the statutory timescale, normally one month from receipt. The Council will only charge a fee where permitted by law. Where a request is complex, manifestly unfounded or excessive, or where clarification is required, the Council will manage the request in accordance with law and ICO guidance.

Searches for personal data must be reasonable and proportionate. However, where relevant personal data may be held in personal email accounts, personal devices or non-corporate communications channels because Council business was conducted there, councillors and staff must cooperate with searches and provide relevant material to the Council.

17. Freedom of information, environmental information and publication

The Council is committed to openness and transparency. It will maintain a Publication Scheme and publish information routinely where required or appropriate, including agendas, minutes, financial information, policies, councillor information and other records of public interest.

The Freedom of Information Act 2000 applies to recorded information held by the Council, or held by another person on behalf of the Council. The Environmental Information Regulations 2004 apply to recorded environmental information held by, or for, the Council. These regimes can apply regardless of whether information is held in a Council mailbox, personal email account, messaging account, personal device or other system.

Requests for information must be forwarded to the Clerk / Proper Officer immediately. The Council will respond within statutory timescales and will apply exemptions or exceptions only where legally justified.

18. Meetings, openness and confidential business

Formal meetings of the Council and its committees will be publicised in accordance with statutory requirements. Agendas, reports, background papers and minutes will be made available as required by law and Council procedures.

The Council or a committee may resolve to exclude the press and public where confidential or exempt information needs to be considered, for example staffing matters, personal information, legal advice, contractual negotiations, commercial sensitivity or other matters where public discussion would not be appropriate. Reasons for exclusion will be recorded.

The public and press may film, photograph, record or report on meetings open to the public, subject to orderly conduct and lawful safeguards. The Council will take reasonable steps to protect children, vulnerable people and members of the public who object to being filmed, while preserving transparency and the proper conduct of meetings.

Written records will be kept of officer decisions where required by the Openness of Local Government Bodies Regulations 2014 and Council procedures.

19. Data transparency

The Council will comply with the Local Government Transparency Code 2015 where the Code applies to the Council, and will have regard to transparency expectations as good practice where appropriate. Public data should be published in a timely, accessible and reusable format where practicable, while protecting personal data, confidential information and information subject to legal exemptions.

Transparency does not override data protection, confidentiality or legal privilege. Before publishing information, the Council will consider whether redaction, anonymisation or withholding is required.

20. Disclosure and Barring Service information

Where the Council undertakes DBS checks, it will comply with DBS requirements and the DBS Code of Practice in relation to the secure storage, handling, use, retention and disposal of certificates and disclosure information. DBS information will be accessed only by authorised persons and retained only for as long as necessary and lawful.

21. Direct marketing, consultations and electronic communications

The Council will comply with data protection law and the Privacy and Electronic Communications Regulations when sending electronic communications, newsletters, consultation updates or marketing-style messages. Consent, soft opt-in or another applicable lawful basis will be used where required. Individuals will be given clear information about how to opt out where appropriate.

Council contact lists must not be used for party political, electoral, personal or commercial communications.

22. Complaints

Individuals may complain to the Council about how their personal data has been used, how an information rights request has been handled, or how this policy has been applied.

Complaints should be sent to the Clerk / Proper Officer through the Council's published contact details. The Council will acknowledge data protection complaints within 30 days and respond without undue delay. The Council will keep a record of the complaint, assessment, response and any remedial action.

If an individual remains dissatisfied, they may complain to the Information Commissioner's Office. The ICO can be contacted through its website or by telephone on 0303 123 1113. Individuals should normally raise the issue with the Council first so that the Council has an opportunity to investigate and respond.

23. Personal data breaches and information incidents

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include sending an email to the wrong recipient, losing paperwork, use of a non-Council email to communicate with any third party in relation to council matters, disclosing addresses, unauthorised access, use of a non-Council email to communicate with residents regarding council matters, ransomware, theft of a device, accidental publication or failure to use bcc where required.

All councillors, staff, volunteers and contractors must report any actual or suspected breach immediately to the Clerk / Proper Officer. Reports must not be delayed while further enquiries are made.

The Council will assess each incident, take containment and remedial action, keep a breach record and notify the ICO within 72 hours where required by law. Where a breach is likely to result in a high risk to individuals, the Council will inform affected individuals without undue delay unless an exemption applies.

24. Training, awareness and compliance

The Council will provide proportionate data protection and information governance induction, guidance and refresher training to staff and councillors. Training will cover this policy, email and device use, subject access, FOI/EIR, breach reporting, confidentiality and records management.

Councillors and staff are expected to read this policy, follow Council procedures and seek advice from the Clerk / Proper Officer where uncertain. Failure to comply may be managed under the relevant employee disciplinary process, councillor code of conduct process, contract terms or other appropriate procedure.

25. Review

This policy will be reviewed at least annually and sooner where there is a relevant change in law, ICO guidance, Council systems, service delivery, risk profile or operational need. The next scheduled review is May 2027.

Appendix A - Practical handling of requests

Any councillor or member of staff who receives a request that may relate to information rights must forward it to the Clerk / Proper Officer immediately. A request does not need to mention the UK GDPR, data protection, FOI, EIR or subject access to be valid.

Examples of phrases that may trigger this process include:

- "Please send me all information you hold about me."
- "I want a copy of my file."
- "What information do you have about this matter?"

- "Please provide emails about..."
- "I want to know why my data was shared."
- "Please delete my information."
- "Please correct my address/details."

The Clerk / Proper Officer will coordinate logging, identity checks where needed, clarification, searches, exemptions, redactions, approval and response.

Appendix B - Council email and records checklist

Requirement	What this means
Use Council email	Use only your @chigwellparishcouncil.gov.uk account for all Council-related matters.
Do not auto-forward	Do not automatically forward Council email to personal accounts.
Keep records available	File important Council correspondence in the appropriate Council system or ensure it is available to the Clerk / Proper Officer.
Personal email exception	Use personal email only in a genuine emergency or where expressly authorised; then transfer the record to Council systems and notify the Clerk / Proper Officer.
Requests apply everywhere	Council business in personal or political email, messaging accounts or devices may be searched and disclosed under lawful requests.
Separate roles	Do not use Council email or Council data for party political, election, personal or commercial activity.
Report problems	Report mistakes, loss, wrong-recipient emails, suspected phishing or other incidents immediately.