

CROOKHAM VILLAGE PARISH COUNCIL

UK GENERAL DATA PROTECTION REGULATIONS (GDPR) & DATA PROTECTION ACT (DPA)

POLICY AND SCHEDULE OF INFORMATION HELD

1. Introduction

- 1.1 Crookham Village Parish Council is committed to compliance with the requirements of the UK General Data Protection Regulation (2000) and the Data Protection Act 2018 (the Act).
- 1.2 The Council will therefore follow procedures that aim to ensure that all employees, elected councillors, contractors, agents, consultants, partners, or other servants of the Council who have access to any personal data held by, on or behalf of, the Council, are fully aware of and abide by their duties and responsibilities under the Act.

2. Statement of Policy

- 2.1 In order to operate efficiently, the Council must collect and use information about people with whom it works. This may include members of the public, current, past and prospective employees, clients and customers and suppliers. In addition, it may be required by Law to collect and use information in order to comply with the requirements of the Government. This personal information must be handled and dealt with properly, by whatever means it is collected, recorded and used and whether it be on paper, in computer records or recorded by any other means there are safeguards within the Act to ensure this.
- 2.2 The Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

3. The Principles of Data Protection

- 3.1 The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These are legally enforceable.
- 3.2 The Principles require that personal information:
 - 3.2.1 Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
 - 3.2.2 Shall be obtained only for one or more specified and lawful purpose(s) and shall not be further processed in any manner incompatible with that purpose or those purposes.
 - 3.2.3 Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.
 - 3.2.4 Shall be accurate and where necessary, kept up to date.

- 3.2.5 Shall not be kept for longer than is necessary for that purpose or those purposes.
- 3.2.6 Shall be processed in accordance with the rights of data subjects under the Act.
- 3.2.7 Shall be kept secure (protected by an appropriate degree of security).
- 3.2.8 Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Adequacy Regulations: The UK government has confirmed the destination country provides an adequate level of data protection. Current adequate countries include EEA states, Gibraltar, Guernsey, Isle of Man, Jersey, and Switzerland.

UK Extension to EU-US Data Privacy Framework (DPF): As of October 12, 2023, you can transfer data to US organizations that are certified under the UK Extension to the EU-US DPF.

4. **Personal Data & Sensitive Data**

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **sensitive personal data**.

4.1 Personal data is any piece of information that relates to or can be related to a natural person that can directly or indirectly identify them.

- 4.1.1 **Identified or Identifiable:** You are identified if you can be directly named, or identifiable if you can be distinguished from others using identifiers like name, ID number, location, or online ID (e.g., cookie ID, IP address).
- 4.1.2 **Broad Interpretation:** The term "any information" means it covers a vast range of data, including physical, physiological, genetic, mental, economic, cultural, or social identity.
- 4.1.3 **Examples:** Names, email addresses, phone numbers, birth dates, addresses, bank details, photos, voice recordings, and even behavioural data (like browsing habits if linked to you) are personal data.
- 4.1.4 **Indirect Identification:** Information that isn't directly identifying but can be combined with other data to pinpoint an individual (e.g., a postcode combined with a job title) also counts.

4.2 Sensitive personal data is defined as personal data consisting of information as to:

- 4.2.1 Racial or ethnic origin.
- 4.2.2 Political opinion.
- 4.2.3 Religious or other beliefs.

- 4.2.4 Trade union membership.
- 4.2.5 Physical or mental health or condition.
- 4.2.6 Gender.
- 4.2.7 Criminal proceedings or convictions.

4.3 Handling of personal/sensitive information

The Council will:

- 4.3.1 Observe fully conditions regarding the fair collection and use of personal information.
- 4.3.2 Meet its legal obligations to specify the purpose for which information is used.
- 4.3.3 Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- 4.3.4 Ensure the quality of information used.
- 4.3.5 Apply checks to determine the length of time information is held.
- 4.3.6 Take appropriate measures to safeguard personal information.
- 4.3.7 Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

This includes,

- 4.3.8 The right to be informed that processing is being undertaken.
- 4.3.9 The right of access to one's personal information within the statutory 40 days.
- 4.3.10 The right to correct, rectify, block or erase information regarded as wrong information.

5. Implementation

- 5.1 The Clerk to Crookham Village Parish Council is the named Data Protection Officer and is responsible for ensuring adherence with the Act. The schedule of information held is attached.

6. Notification to the Information Commissioner

- 6.1 The Information Commissioner maintains a public register of Data Controllers. The Act requires every Controller to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. Should the Clerk resign the Information Commissioner must be notified immediately and the new Clerk duly registered with that office.

CROOKHAM VILLAGE PARISH COUNCIL

UK GENERAL DATA PROTECTION REGULATIONS (GDPR)

Contact Details: Data Protection Officer - Clerk@crookhamvillage-pc.gov.uk

RECORD TYPE	WHAT PERSONAL INFORMATION IS COLLECTED	CATEGORY OF INDIVIDUAL	LAWFUL BASES	WHERE DOES THE DATA GO	RETENTION PERIOD	START DATE	FINISH DATE	DISPOSAL METHOD & RESPONSIBLE PERSON
Minutes Full Council & Committees	Elected and co-opted Councillors & Staff names	Management	Basis C	Website Onedrive Cloud Computers	Signed hard copy indefinitely	N/A	N/A	Indefinite as per Legislation
Public comments to Planning Apps	Contact details	Management	Basis E	Onedrive Cloud Computers	Refer to Retention & Disposal Schedule	N/A	N/A	Deputy Clerk Redact personal details when comments received.
Website information Facebook page	NONE	N/A	N/A	N/A	Until updated	1 March 2026	Dependent upon updates	Erasure/deletion of out-of-date information (excluding statutory records of Council). Deputy Clerk
Onedrive files On Officers' laptops Councillors & Centre Managers	Contact details	N/A	Basis B	Onedrive	Refer to Retention & Disposal Schedule	N/A	N/A	Retain – Statutory and associated legal documents.
Personal laptop/idpads etc BYOD	Contact details	Management	Basis B	Onedrive	Refer to Retention & Disposal Schedule	N/A	N/A	On cessation of office Cloudy/IT be requested to delete all files.
Hall Hire	Email contact	MoP Enquiries	Basis B	N/A	N/A	N/A	N/A	Delete
Contracts	Contact details	Client	Basis B	One drive & Hard copies	Retain 6 years	From start of hire	6 years	Centre Managers & Deputy Clerk Record and shared Hard copies delete from OneDrive Centre Managers
Casual bookings	Contact details	Client	Basis B	& Lemon Bookings & Quickbooks	Retain 6 years	From start of hire	6 years	
Regular & 6 months Hire Contracts	Contact details	Client	Basis B					

RECORD TYPE	WHAT PERSONAL INFORMATION IS COLLECTED	CATEGORY OF INDIVIDUAL	LAWFUL BASES	WHERE DOES THE DATA GO	RETENTION PERIOD	START DATE	FINISH DATE	DISPOSAL METHOD & RESPONSIBLE PERSON
Contracts: Trees/Lengthsman Grounds Maintenance Caretaker/DGCS Gardwell CCTV Waste Bins/Litter Bins Pest Control Water monitoring Fire Safety Intruder Alarm	Contact details	Management	Basis C	Onedrive Hard copies	Retain whilst current	From start of contract	Refer to document retention schedule	Officer or Manager who engaged contractor periods.
Contracts Insurance	Staff details	Management	Basis C	Cloud	3 years	Renewed annually	Annual	Delete hard copy and online
Payroll & Pensions	Staff details	HR	Basis B & C	HMRC Bank Quickbooks	12 years	N/A	Employment ceases	Where permitted RFO deletes No control over Quickbooks
Feedback at CVPC Website	MoP contact	Management	Basis C	HDC/HCC Cllrs	Whilst current	N/A	N/A	Delete when query responded to.
Legal correspondence	Staff CVPC and legal company	Management	Basis C	Staff and Cllrs	Retain until business concluded	From initial contact	When business concluded	Archive or delete according to the issue
Staff Contracts	Contact details	HR	Basis C	Onedrive & Hard copy	Whilst employed	Start date	Employment ceases	Destroy hard copies delete all on line.
Building Plans	Developer	Management	Basis B	Onedrive Cloud	Lifetime of the building	From acquisition	Disposal Plus 6 years	Delete Clerk
Employers Liability Insurance	N/A	Management	Basis B	Onedrive Cloud	40 years	From commencement	40 years	Delete Clerk
Insurance contracts	Staff & Broker	Management	Basis B	Onedrive Cloud	3 years	From commencement	3 years	Delete Clerk
Councillor DPI & Acceptance of Office	Name address financial interests	Statutory	Basis C	Onedrive Website	N/A	Election or Co-opt date	Cessation of office	Delete online and destroy hard copies Clerk
NB DISPOSAL METHOD 1. SECURE DELETION – for general data 2. ARCHIEVING – transferring Council Minutes and historically significant records to relevant bodies 3. HARD COPY – shredding by reputable company and keeping a record 4. DEVICES - DESTROY								
Breakthrough advice: Personal – anything that identifies someone, data must relate to the individual Data Controller – Parish Council								

Data Processor – usually supplier
Data sharing – should have a Code of Practice to cover transmission and/or disseminations
Special Category Data – race, religion, age, disability, gender etc
Data Subject – data relates to
Data transfer – going out of UK – EU 2020 list advises of countries considered compliant with GDPR
Consent – clear yes or no
Data breach – 72 hrs to report to ICO (Data loss/breached/hacked (unauthorised access))

The 6 Lawful Bases

What are the lawful bases for processing? The lawful bases for processing are set out in Article 6 of the UK GDPR. At least **one** of these must apply whenever you process personal data:

(a) Consent:

the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract:

the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation:

the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests:

the processing is necessary to protect someone's life.

(e) Public task:

the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests:

the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)