Chaddleworth Parish Council

Data Map

Version number	1.0		
Adopted by	Full Council		
Date adopted	13th January 2026	Review due	Each annual meeting

Overview:

1. This data map is maintained for the Chaddleworth Parish Council Data Protection Policy.

2. Introduction: This data map is simple table that records each Purpose the council has for processing personal data. It shows the types of personal data involved, whether the data is shared with other organisations or handled by data processors on the council's behalf. It also records the lawful basis which allows the council to process the data and identify if any special category data is being processed.

3. Explanation for attributes:
   i. By category of individual or one within an entity (Council, Staff, Residents, Contractors, Correspondence, Applicants).
   ii. Purpose – why the data is used (e.g. recording minutes, managing payroll).
   iii. Source – from where the data was obtained (e.g. data subject, controller).
   iv. Data Held – The categories of personal which are held. For example, contact information, bank details.
   v. How Held – covers categories of processors, e.g. any companies or people who process data for the council, but don't decide how it's used. For example, a website host, an email provider, and a cloud software provider (names of third countries or international organisations that personal data is transferred to, identify whether data is processed outside the UK, and if so, where).
   vi. Basis – the reason that the data is held (e.g. legal requirement, legitimate interest).
   vii. Retention Period – how long the data is available before deletion.
   viii. Where Data Shared – who the data is shared with, outside the council (e.g. data controllers such as HMRC).
   ix. Why Shared – the reason that the data is shared.

4. This Data Map proceeds to a Risk Assessment by Purpose.

Data Map:

5. Individual/Entity: **Councillor**

Purpose:	Councillor	**Source:**	Councillor	#3.1
Data Held:	Contact information	**How Held:**	Electronically with 2FA cloud.	
Basis:	Legal obligation	**Retention Period:**	For the duration as Parish's Councillor	
Shared With:	None	**Why Shared:**		
Notes:	Electronically with 2FA cloud is via legal entity Google Ireland Limited which within the EU adheres to UK and EU regulations including GDPR.			

Purpose:	Councillor's Register of Interests	**Source:**	Councillor	#3.2
Data Held:	Completed form	**How Held:**		
Basis:	Legal obligation	**Retention Period:**	For the duration as Parish's Councillor	
Shared With:	Local Authority, Monitoring Officer	**Why Shared:**	for legal obligation	
Notes:	Potentially includes 'Special Category Data' the inclusion which is required for 'Substantial public interest conditions' and for which the Chaddleworth Parish Council GDPR Appropriate Policy Document (CPC GPPR APD) checks that the data is protected.			

Purpose:	DCLG Transparency Code	**Source:**	Clerk	#3.3
Data Held:	Name	**How Held:**	In Council minutes and on Parish website	
Basis:	Legal obligation	**Retention Period:**	In perpetuity in minutes, for the duration as Parish's Councillor on website	
Shared With:	CPC	**Why Shared:**	Electronically on the Parish Council website. On paper in the Minute Books, lodged at the Royal Berkshire Archives	
Notes:				

Purpose:	To record the approval of Council minutes	**Source:**	Clerk	#3.4
Data Held:	Signature	**How Held:**	In physical record of Council minutes.	
Basis:	Legal obligation	**Retention Period:**	In perpetuity.	
Shared With:	CPC	**Why Shared:**	On paper in the Minute Books, lodged at the Royal Berkshire Archives	
Pertaining Notes:				

6. Individual/Entity: **Staff (in particular being the Clerk and RFO)**

Purpose:	Recruitment	**Source:**	Council	#4.1
Data Held:	CV and covering letters by Job Applicants	**How Held:**	Electronically with 2FA cloud.	
Basis:	Legal obligation	**Retention Period:**	For 6 months after completion of the recruitment process or after notifying unsuccessful applicant/s (whichever is earlier)	
Shared With:	None	**Why Shared:**		
Notes:	Electronically with 2FA cloud is via legal entity Google Ireland Limited which within the EU adheres to UK and EU regulations including GDPR.			

Purpose:	Employment	**Source:**	Council	#4.2
Data Held:	Contract, name, address, DoB, NI number	**How Held:**	Electronically with 2FA cloud.	
Basis:	Legal obligation	**Retention Period:**	Until 6 years after employment has ceased	
Shared With:	HMRC	**Why Shared:**	HMRC basic PAYE tools	
Notes:	Current clerk has declined Pension arrangements. Electronically with 2FA cloud is via legal entity Google Ireland Limited which within the EU adheres to UK and EU regulations including GDPR.			

Purpose:	Salary	**Source:**	Council	#4.3
Data Held:	Bank details	**How Held:**	Within CPC bank account	
Basis:	Legal obligation	**Retention Period:**	For duration of employment	
Shared With:	None	**Why Shared:**		
Notes:	Currently Metro Bank.			

7. Individual/Entity: **Residents**

Purpose:	The verification of elector eligibility for nominations and co-option	**Source:**	Local Authority	#5.1
Data Held:	Register of Electors within the Parish	**How Held:**	Electronically with 2FA cloud.	
Basis:	Public task	**Retention Period:**	As each register issued, delete previous	
Shared With:	None	**Why Shared:**		
Notes:	Electronically with 2FA cloud is via legal entity Google Ireland Limited which within the EU adheres to UK and EU regulations including GDPR.			

8. Individual/Entity: **Applicants**

Purpose:	The processing of an application for a grant	**Source:**	Applicant	#6.1
Data Held:	Name, email, phone, address, bank account	**How Held:**	Electronically with 2FA cloud.	
Basis:	Public task	**Retention Period:**	6 years following the end of the financial year	
Shared With:	None	**Why Shared:**		
Notes:	Bank account details held where grant given currently Metro Bank. Electronically with 2FA cloud is via legal entity Google Ireland Limited which within the EU adheres to UK and EU regulations including GDPR.			

Purpose:	The processing of an application for waitlist for parish affordable housing	**Source:**	Applicant	#6.2
Data Held:	Name, email, phone, address, family details	**How Held:**	Electronically with 2FA cloud.	
Basis:	Public task	**Retention Period:**	Renewed annually, deleted if not reviewed after two renewal requests	
Shared With:	Local Authority	**Why Shared:**	When an affordable home (Schedule 106) becomes available for the purposes of this being awarded suitably	
Notes:	Bank account details held where grant given currently Metro Bank. Electronically with 2FA cloud is via legal entity Google Ireland Limited which within the EU adheres to UK and EU regulations including GDPR.			

9. Individual/Entity: **Correspondent**

Purpose:	To receive and respond to correspondence	**Source:**	Member of the public	#7.1
Data Held:	Name, email, potentially further details including phone and address.	**How Held:**	Electronically with 2FA cloud.	
Basis:	Public task	**Retention Period:**	Deleted if after two years of initial correspondence	
Shared With:	Correspondence may be shared with Councillors	**Why Shared:**	To support resolution	
Notes:	Email service is provided via HugoFox.			

10. Individual/Entity: **Contractor**

Purpose:	Services requested and provided	**Source:**	Contractor	#8.1
Data Held:	Name, contact details, invoices, bank details	**How Held:**	Electronically with 2FA cloud.	
Basis:	Contract	**Retention Period:**	6 years following the end of the financial year	
Shared With:	None	**Why Shared:**		
Notes:	Currently Metro Bank.			

Risk Assessment by Purpose:

Purpose:	**3 Councillor**	**4 Staff**	**5 Residents**	**6 Applicants**	**7 Correspondent**	**8 Contractor**
Residual risk (low, medium or high)	Low	Low	Low	Low	Low	Low
Risk Safeguard (accept/mitigate)	Accept	Accept	Accept	Accept	Accept	Accept
Safeguard Notes						
Data stored securely	Yes	Yes	Yes	Yes	Yes	Yes
Data held on personal devices	*digital	*digital	*digital	*digital	*digital	*digital
Data kept longer than needed?	No	No	No	No	No	No
Data correct and kept up to date?	Yes	Yes	Yes	Yes	Yes	Yes
Are data processors used?	Yes	Yes	Yes	No	Yes	Yes
Are there contracts in place with them?	Yes	Yes	Yes	N/A	Yes	Yes
Data published online?	Yes	Yes	No	No	No	No
Is data transferred internationally?	*digital	*digital	*digital	*digital	*digital	*digital
Can individuals exercise their rights easily if they ask?	Yes	Yes	Yes	Yes	Yes	Yes
Can requests for access, rectification, or deletion be handled appropriately?	Yes	Yes	Yes	Yes	Yes	Yes
Are new or changing systems (websites, apps, surveys) being risk assessed at the start?	Yes	Yes	Yes	Yes	Yes	Yes

*digital = Bank account details where held are currently with Metro Bank. Storage is electronically with 2FA cloud is via legal entity Google Ireland Limited which within the EU adheres to UK and EU regulations including GDPR. Email and Website service is provided via HugoFox.

Data Map Process Description:

11. Data Map Checklist:
    i. Identify recipients and providers of council functions and services (Council, Staff, Residents, Contractors, Correspondence, Applicants).
    ii. For each function or service, list the purpose(s) for processing personal data (e.g. producing minutes, administering allotments, etc).
    iii. For each purpose, complete a sub-table in the data map.
    iv. Identify any data controllers for each purpose (i.e. organisations or persons the council shares data with), such as HMRC, banks, or other local authorities.
    v. Identify any data processors for each purpose (i.e. suppliers that process the council's data on their behalf), such as website hosts, cloud storage providers, email services, payroll providers, etc.
    vi. Identify where any data leaves the UK (international transfers), which is common with cloud-based systems, and will require additional safeguards.

12. Process: Address each of the following as part of the data mapping process, giving regard to the data protection principles of data minimisation and storage limitation:
    i. An explanation why this data is held for the Council's purposes.
    ii. That a minimum of data is held, securely, and for no longer needed than needed.
    iii. Each purpose in the data mapped has a lawful basis.
    iv. Where special category data has been identified, the lawful basis for processing, the additional condition to process, and, where needed, the Appropriate Policy Document (APD) is noted.

13. Basis: There are six lawful bases (plural of basis) that can be used to process personal data, and each has requirements (UK GDPR Article 6(1)).
    i. Consent – When an individual makes a fully informed decision to agree to processing freely and takes a positive action to demonstrate that consent. Example: a resident signing up for a council newsletter.
    ii. Contract – When data is needed to deliver a contract that the council has entered into, or when someone wants to have a contract with the Council (e.g. an allotment tenancy).
    iii. Legal obligation – Where the law requires the Council to process data (e.g. a councillor's register of interest).
    iv. Vital interests - When processing is necessary to protect someone's life (e.g. sharing health information with medical professionals if the person is unable to make decisions for themselves. Note: This is rare for councils to use).
    v. Public task – Where processing is necessary for a task carried out in the public interest, or in the exercise of official authority given to the council, but there is no legal requirement to do it (e.g. answering general correspondence).
    vi. Legitimate interests – Can be used when no other lawful bases apply, but it requires an additional risk assessment. The assessment is a three-part test, and the ICO provides a downloadable template to help with this (e.g. CCTV in council buildings, rely on this basis if your processing passes the three-part test).

14. Special Category Data: Some personal data needs additional safeguards which are classed special category data. This includes personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health, sex life and sexual orientation. This may occur in routine tasks. Examples include: a resident includes details about their disability in a request for an accessible allotment plot; a staff file records health information, or trade union membership; a councillor lists their role on a church council in their Register of Interests, which indirectly reveals

their religious belief. When special category data is identified for a purpose, an extra safeguard must be in place to allow that processing. This safeguard is called an additional condition to process.

i. Data protection law requires that special category data be processed only if there is both a normal lawful basis and an additional condition.
ii. Some additional conditions also require an Appropriate Policy Document (APD) to explain how the data is protected.
iii. Example of a special category data in practice: A councillor lists their role on a church council in their Register of Interests, which reveals their religious belief. Lawful basis = Legal obligation (the council is required by law to publish the register); Additional condition = special category data (Substantial public interest conditions, Statutory and government purposes). Appropriate Policy Document required = Yes (an ADP is needed).

15. Rights: Individuals have legal rights over their personal data, as set out in UK GDPR Articles 13 to 23. Chaddleworth Parish Council recognises these rights. Individuals have the right to:
    i. Be informed – To know how and why their data is used, what their rights are and how they can complain.
    ii. Request access – To request a copy of their data (Subject Access Requests).
    iii. Request rectification – To have inaccurate or incomplete data corrected.
    iv. Request erasure – To request deletion of their data in certain situations.
    v. Request restriction – To limit how data is processed.
    vi. Request data portability – To have their data transferred to another data controller.
    vii. Object – Individuals can object to how their personal data is used. If they are not satisfied with the response, they can raise their concern with the ICO, or in some cases, take it to court.
    viii. Request review of automated decisions – Not to be subject only to decisions made by computers (including profiling) if the decision has a negative effect. They can ask for such decisions to be reviewed by a human.

16. Risk Assessment: by purpose, assess risk:
    i. Is data stored securely (For example, locked cabinets, password protection, multi-factor authentication, up-to-date computer equipment, etc)?
    ii. Is data held on personal devices?
    iii. Is the data correct and kept up to date?
    iv. Is data kept longer than needed?
    v. Are data processors used (i.e. payroll providers, website hosts, IT support)?
    vi. Are there contracts in place with them?
    vii. Is the data published online?
    viii. Is data transferred internationally?
    ix. Can individuals exercise their rights easily if they ask?
    x. Can requests for access, rectification, or deletion be handled appropriately?
    xi. Are new or changing systems (websites, apps, surveys) being risk assessed at the start?
    xii. The formal tool for this is a Data Protection Impact Assessment (DPIA). The ICO only requires DPIAs for activities that are likely to be high risk
    xiii. For each purpose, the risk is assessed with notes on mitigations or acceptance.

17. Data review: This data will be reviewed at least annually to ensure its relevance and effectiveness.

18. Glossary
    i. *Appropriate Policy Document (APD)* A short written document that explains how the council will protect and manage special category data. It must describe how you comply with the data protection principles and how long you keep information.
    ii. *Data Breach* An incident where personal data has its confidentiality lost, its integrity damaged, or its availability removed — whether by accident or on purpose. Data breaches can vary significantly in scale, from small incidents to major catastrophes. It is essential for councils to maintain records if them to identify patterns and prevent future errors.
    iii. *Data Controller* A person or an organisation that decides why and how personal data is used. The council will be a data controller, and it's common for councils to share data with other data controllers, e.g. passing employee payroll data to HMRC.
    iv. *Data Map* A record of processing activities (often a table or spreadsheet) that sets out what personal data the council holds, why it is used, where it is stored, who can access it, and how long it is kept. The detailed and well-thought-out data map is the foundation for all other data protection work.
    v. *Data Processor* An external company or person that processes personal data on the council's behalf, but does not decide how it is used. Examples include email providers, payroll providers, website hosts, or cloud storage companies. Councils must have a written contract in place with processors that set outs requirements and obligations to comply with data protection law.
    vi. *Data Protection Impact Assessment (DPIA)* A structured risk assessment that helps the council think through how an activity affects people's privacy, what risks might arise, and what mitigations can be put in place to reduce the risks identified.
    vii. *Data Protection Officer A data protection officer (DPO)* is a formal position appointed for compliance monitoring, providing independent advice, and acting as a contact point. Parish councils are normally exempt from the requirement to appoint a DPO. Note: In rare cases where a parish council is regularly monitoring individuals or undertaking large-scale processing of special category or criminal convictions data, then a DPO may still be required.
    viii. *Data Subject* Any individual whose personal data is being processed. This could be anyone, including staff, councillors, contractors, and residents.
    ix. *Personal Data* Any information that identifies a living person, either directly (e.g. name) or indirectly (e.g. job title, reference number, or photo). Ask yourself, can this information identify who the person is? If yes, it's personal data.
    x. *Processing* Anything you do with personal data, including collecting, using, storing, sharing, publishing, or deleting it. If you handle personal data in any way, you are processing it.
    xi. *Purpose* The reason personal data is being used. Examples include (but are not limited to) keeping minutes, paying staff, or running an allotment. A council will have multiple different purposes.
    xii. *Special Category Data* A type of personal data that is more sensitive and needs extra protection. It includes personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health, sex life and sexual orientation.
    xiii. *Lawful Basis* The legal reason for processing personal data under the UK GDPR (Article 6). Every purpose in your data map must have a lawful basis assigned to it and recorded.
    xiv. *Privacy Notice* A single public-facing document, tailored to the council, that explains in plain English what personal data the council processes, why it is used, how long it will be kept for, how to complain and what rights people have.
    xv. *Rights Requests* Requests made by individuals to exercise their data protection rights, such as access, correction, or deletion. Requests can be made to the council verbally or in writing, without the need to contact a specific person or use a form. These requests must be dealt with by the council promptly and within a timeframe of usually one month.