



Upwood and the Raveleys Parish Council

Data Protection Manual

Introduction

The key objective of this policy is to provide Upwood and the Raveleys Parish Council with a simple framework which will govern decisions on whether a document should be retained or disposed of. In the case of documents which are to be retained by Upwood and the Raveleys Parish Council the Policy includes guidance on the format in which they should be retained and appropriate retention periods.

Implementation of the policy should save staff time when retrieving information, by reducing the amount of information that may be held unnecessarily.

The policy clarifies the different roles of staff in relation to document retention and disposal in order that they understand their responsibilities, and who to refer to if they are unsure about any document and require clarification.

It is envisaged that this Policy will assist the Parish Clerk in securing compliance with legal and regulatory requirements, including the COSHH Regulations 2002, the Freedom of Information Act 2000, the Environmental Information Regulations 2005, the Data Protection Act 2018 and the Code of Practice on the Management of Records under Section 46 of the Freedom of Information Act 2000. In addition to assisting officers in their day to day business, this should also ensure that searches for information requested under the Freedom of Information legislation are as quick as possible.

Additionally, the Policy should help to ensure that Upwood and the Raveleys Parish Council archives, records and documents that are of historical value appropriately for the benefit of future generations.

Scope

This Document Retention Policy applies to all information held by Upwood and the Raveleys Parish Council and its external service providers where they are processing information on Upwood and the Raveleys Parish Council's behalf.

Policy Statement

The Parish Clerk will ensure that information is not kept longer than is necessary and will retain the minimum amount of information that it requires to carry out its' statutory functions and the provision of services.

Retention and Disposal Policy

Decisions relating to the retention and disposal of documentation should be taken in accordance with this Policy, in particular:

- Disposal and Retention Considerations – a checklist to be followed where the disposal of any document is being considered and comprehensive guidance on the recommended and statutory minimum retention periods for specific types of documents and records. See Upwood and the Raveleys Parish Council's Management of Record and Retention of Documents Policy¹.

In circumstances where a retention period of a specific document has expired, a review should always be carried out prior to a decision being made to dispose of it. This review should not be particularly time consuming and should be straightforward. If the decision to dispose of a document is taken, then consideration should be given to the method of disposal to be used.

Roles and Responsibilities

The Parish Clerk will be responsible for determining (in accordance with this Policy) whether to retain or dispose of specific documents within the remit of their service area.

The role of Data Protection Officer will be seconded to Priviness Ltd.

Disposal

Confidential waste documents should be stored securely pending destruction in a secure storage area within Upwood and the Raveleys Parish Council offices. It is essential that any documents which are to be thrown away and contain confidential or personal data must be disposed of in the correct way, to avoid breaches of confidence or of the Data Protection Act 2018.

Processes and Procedures

Data Subject Rights Process

Legal Warning

Personnel are reminded that knowingly altering or erasing data which is the subject of a “data subject access request” under Articles 13 & 14 of GDPR is a criminal offence.

Responsibility

Responsibility for ensuring the rights of data subjects are respected and responded to in a timely and appropriate way lies with the Parish Clerk of Upwood and the Raveleys Parish Council.

Day to day management of subject rights is to be delegated to the Parish Clerk.

Data Management Team

Composition: Individual staff may be appointed or removed from participation in the Data Management Team as considered necessary by the Parish Council. Initially the Data Management Team will consist of:

Parish Clerk– parishclerk@upwood.org

Data Protection Officer – info@priviness.eu

All staff will be informed that any request they receive which might be related to data subject rights should be forwarded to the email address above.

Duties of the Data Management Team

See Upwood and the Raveleys Parish Council Information and Data Protection Policy²

Receipt and log of requests see: Upwood and the Raveleys Parish Council Data Breach and Reporting Form³ Re-adopted March 2020 covered by Upwood and the Raveleys Parish Council Complaints Procedure⁴ Re-adopted May 2019

Actions on receipt of an enquiry

When informed of a potential request the Data Management Team will:

- Log the enquiry in the Data Subject Request Log
- Determine if the enquiry is a request under the data subjects’ rights
- Determine if an extension to the deadline is required
- Decide on the redaction policy

- Delegate responsibility for actions and set deadlines for completion
- Update the Data Subject Request Log
- Monitor performance of actions

Identification

Principles:

Upwood and the Raveleys Parish Council will not adopt a pre-set standard for the level of proof of identity required of a data subject.

The Data Management Team will decide if the requestor has the right requested and, if not, whether there is a compelling reason to refuse the request. This decision will be documented and recorded in the Data Subject Request Log.

Reasons a requested right may not be available include but are not limited to:

- Upwood and the Raveleys Parish Council has a legal obligation to retain data that they are requested to erase.
- Data does not constitute “Personal Data” as defined by Article 4 (1) of GDPR.
- Release of the data would adversely affect the rights and freedoms of others.
- A DPIA or Balancing Test has been conducted which establishes the interest of Upwood and the Raveleys Parish Council in processing the data outweigh the risks to the rights and freedoms of the subject who has objected to the processing, requested restriction of processing or erasure of the data.
- Request is manifestly unfounded or excessive (in particular because of the repetitive character of the request) as per Article 12 (5) of GDPR and subject refuses to pay a reasonable fee.

However, even where it is determined that the subject does not have an enforceable right the request will nevertheless be considered by the Data Management Team and reasons for refusal will be documented.

Refusal of request

Manifestly Unfounded Request

A request is manifestly unfounded where it “very obviously has no basis and is unjustified”. In such a case a reasonable administration fee may be charged. The reasons for making this decision should be documented and may include:

- Lack of an existing relationship with the subject and no reasonable cause to believe Upwood and the Raveleys Parish Council holds data about the subject.
- Known antagonistic relationship or grudge.
- Data requested does not satisfy the definition of personal data as per Article 4 (1) of GDPR.
- Request is part of a repetitive pattern.
- Request is clearly a “fishing expedition”.

Where a request is judged Manifestly Unfounded the subject must be informed of the reasons for this decision **and** the proposed fee.

Excessive Request

Subject requests are to be considered a normal part of business since the advent of GDPR and therefore Upwood and the Raveleys Parish Council should not be expecting to charge an administration fee for most requests.

Given the above, the fact that there are costs in terms of the time for staff to administer the rights process and collect or erase data or otherwise act to satisfy the request will not be considered excessive for most requests.

It would be reasonable to assume that a request would require in total several hours of time spread among several staff of different levels of authority (and therefore expense). However, a total of up to half a day (nominally 4 hours) would be unexceptional and therefore non-chargeable.

An “excessive” request would be a request which considerably exceeded the above i.e. would require more than (perhaps) one day of staff time. Likely reasons include:

- Large volume of data
- Data requires extensive redaction
- Data not on live systems (back-up tapes, archives, etc)
- Request includes hard copy data
- Nature of data requires specialised search techniques

Note that an excessive request still needs to be met if the subject is prepared to pay a reasonable administration fee. Such a fee should reflect the real costs of meeting the request which should be documented to the extent possible.

Where a request is judged excessive the subject must be informed of the reason for this decision.

As a general policy a judgement that a request is excessive should be presented to the data subject in a cooperative way and viewed as the beginning of a potential negotiation as to what data could reasonably be provided free of charge or what data could be excluded to reduce the administration fee.

Adverse Effect on the Rights and Freedoms of Others

Complete redaction of all data about any natural person other than the data subject would frustrate the intent of Article 15 of GDPR (Right of Access).

Therefore, it should not be considered that wherever data about another natural person is included in the data requested this should necessarily be redacted. Data should only be redacted where it could have an adverse effect on the rights and freedoms of others.

Consent may be sought to release data even if there is a high risk of adverse effects.

Factors which may lead to a conclusion that a data item may have an adverse effect:

- Data could result in discrimination or physical harm e.g. racial or ethnic origin, religious or philosophical beliefs, health (disabilities), criminal convictions.
- Data relates to a child or vulnerable person.
- Data relates to a politically exposed person, high net worth individual or notable public figure.
- Release of data would likely be regarded by the other natural person as unwarranted or intrusive.
- Data is relevant to a current or likely legal action.
- Known facts regarding the relationship between the data subject and the other person.

Factors which may lead to a conclusion that a data item may **not** have an adverse effect:

- Other person was party to the original communication in which the data is included e.g. other person’s email addresses in “To” list of emails.
- Data is already publicly available e.g. organisation directorships listed at Companies House.
- Data is of very low risk e.g. name or email address.
- Data subject was in possession of the data at some previous time.

Deadline

Initial Deadline

On receipt of a request the Data Management Team will determine the initial deadline for satisfying the request according to the following criteria:

The deadline will be one calendar month from receipt of the request unless criteria 2, 3 or 4 apply e.g. request received: 25 March, deadline: 25 April.

Date obtained by adding one calendar month to date of receipt of request falls on a non-working day (weekend or bank holiday) then next working day e.g.

request received: 25 March, add one calendar month: Sunday 25 April, deadline: Monday 26 April

Date obtained by adding one calendar month to date of receipt does not exist then last day of month e.g.

request received: 30 January, add one calendar month: 30 February, deadline: 28 February

Date obtained from criteria 3 falls on a weekend or bank holiday e.g.

request received: 31 January, add one calendar month: 31 February, last day of month: Saturday 28 February, next working day: Monday 2 March, deadline: 2 March

Extension

On receipt of a request the Data Management Team will determine if it is reasonable to extend the deadline for satisfying the request by a further two months according to the complexity of the request and if it is decided an extension is appropriate the Data Management Team will document the rationale for this decision and inform the data subject.

The extended deadline will be calculated in the same manner as the initial deadline.

Redaction policy and process

Redaction Policy

Covered by Upwood and the Raveleys Parish Council's Information and Data Protection Policy²

Approval of communications with the data subject

Staff shall be informed that all communications with the data subject must be approved by the Parish Clerk.

Breach Process

Personal Data Breach Process

All Employees/Staff, Members, contractors or temporary personnel are responsible for reporting any personal data breach to the Parish Clerk:

Name: Carol Bilverstone

Telephone: 01487 812447

Email: parishclerk@upwood.org

See: Upwood and the Raveleys Parish Council's Data Breach Reporting Form ⁵.

Breaches shall be recorded on Upwood and the Raveleys Parish Council's Personal Data Breach Log⁶.

Personal Data – Subject Access Request Form

Please complete this form if you would like us to supply you with a copy of the personal data which we hold about you. You are entitled to receive this information under Data Protection Legislation.

Once completed, please return this form to Upwood and the Raveleys Parish Council Data Management Office at:
Upwood and the Raveleys Parish Council
9 Meadow Road
Upwood
Huntingdon
Cambridgeshire
PE26 2QJ
parishclerk@upwood.org

We will record this request on Upwood and the Raveleys Subject Access Request Log and endeavour to respond promptly to your request and in any event within one month of the latest of the following:

- Our receipt of this request; or
- Our receipt of any further information from you, which is required to enable us to consider your request.

If, once you have received the requested information, you have any queries or comments, you should contact the Data Management Team at the above postal address or email.

Person the request relates to:

Full name:

Date of Birth:

Address:

.....

Other relevant addresses during the period to which the personal information relates

.....

.....

Email address

Telephone

These details will only be used for the purpose of dealing with your request.

Information requested:

If possible, restrict your request to an incident. Please include timeframes, dates, names or types of documents, any file reference and any other information that may enable us to locate your information, for example, for emails, the names of senders and recipients and approximate dates.

.....
.....
.....
.....

.....
.....

Method by which the information is to be sent:

Please confirm how you wish the personal information to be provided to you, by:

- post at the address provided above
- email at the email address provided above

These details will only be used for the purpose of dealing with your request, including sending the information and any required passwords.

Supplemental Information:

Would you just like to receive the above information, or would you like the following supplemental information (please tick all that apply):

- the purposes of processing your personal information
- the categories of personal information processed by us
- the categories of recipients to whom we disclose your personal information
- the envisaged retention period for your personal information
- automated decision-making, including profiling, to which your personal information is subject
- the source of your personal data, if known

If you believe the information, we hold about you is incorrect, you have the right to ask us to rectify or erase your personal information, to object to its processing or to restrict its processing.

If you are not satisfied with the way in which we have handled your complaint, please contact our Data Management Team at parishclerk@upwood.org.

If we are unable to resolve the issue to your satisfaction, you have the right complain to the Information Commissioner.

Please be aware that if you provide false or misleading information, you may be committing a criminal offence.

I, confirm that the information provided on this form is correct and that I am the individual whose name appears on this form. I understand that Upwood and the Raveleys Parish Council may confirm proof of identity and that it may be necessary to contact me again for further information to locate the personal information I want. I also understand that my request will not be valid until all of the information requested is received by Upwood and the Raveleys Parish Council.

Signed: Dated:

Personal GDPR Covenant

Councillors and Staff

General

- Personal information means any information relating to a living, natural person, who can be identified either directly or indirectly. Processing personal information includes the obtaining, handling, processing, transporting, storing, destruction and disclosure of personal information.
- Upwood and the Raveleys Parish Council will use the personal information of individuals fairly, lawfully, transparently and in a manner consistent with its valid public interests and at the same time, respecting the fair and lawful privacy requirements of those individuals concerned.
- Personnel who have access to, or use personal information about other people as part of their employment or parish duties (for example, parishioner or supplier personal information) must comply with Upwood and the Raveleys Parish Council's policies and procedures for processing personal information.

Data

- Any personal data held is kept securely
- Personal information is not disclosed orally, in writing, accidentally or otherwise to any unauthorised third party.
- Personal information is not transferred internationally without checking that the right safeguards are in place.
- Any portable or mobile ICT equipment or removable storage media is not left in unattended vehicles. Where this is not possible, it must be locked out of sight.
- Passwords and logon information are not disclosed to anyone else.
- Personal information is kept in a locked filing cabinet or locked drawer, or if it is computerised, be password protected, or if kept temporarily on portable media be password protected and kept securely.
- If you are aware of a breach of security with passwords or logon information the parish clerk or the data protection officer must be informed immediately.
- Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct. Any **deliberate** or **serious** breach of this Data Protection Policy by a member of staff may lead to dismissal and even to criminal prosecution.
- Only those personnel who strictly require access to personal information for their role should have such access, and they must ensure that personal information is not shared with personnel who do not need to see it.

Email

- Email to addresses outside the "@upwood.org" domain should not include personal data beyond simple contact information (name, email, telephone, address, job title and place of work).
- Emails sent from "@upwood.org" addresses to "@upwood.org" addresses are restricted to the secure environment and may include personal data.
- Personal information must not be included in the "Subject" field of email regardless of the recipient, do not include names or other potential identifiers.
- Personnel should preferentially use "Bcc". "Cc" should only be used where it is necessary for all recipients to see replies.
- When using distribution lists to send emails outside the organisation always use the "Bcc" facility so that email addresses are not displayed and shared.
- Personal data should only be retained for as long as necessary. The retention periods can differ based on the type of data processed, the purpose of processing or other factors.

All personnel must confirm in writing/via email to the parish clerk that they have read this manual and its attachments, that they undertake to adhere to these policy procedures and abide by the "Councillors and Staff GDPR Covenant".

This document is to be read and utilised in conjunction with the following policies and attachments:

¹Upwood and the Raveleys Parish Council's Management of Records and Retention of Documents Policy. Re-adopted May 2019.

²Upwood and the Raveleys Parish Council Information and Data Protection Policy. Re-adopted March 2020

³Upwood and the Raveleys Parish Council Data Breach and Reporting Form. Re-adopted March 2020

⁴ Upwood and the Raveleys Parish Council Complaints Procedure. Re-adopted May 2019

⁵Upwood and the Raveleys Parish Council's Data Breach Reporting Form.

⁶Upwood and the Raveleys Parish Council's Personal Data Breach Log