Information Protection Policy

UFFORD PARISH COUNCIL

Judi Hallett
CLERK, UFFORD PARISH COUNCIL

Purpose

1) Information is a major asset that Ufford Parish Council has a duty and responsibility to protect.
2) The purpose and objective of this Information Protection Policy is to specify the means of information handling and transfer within the Council.

Scope

1) The Information Protection Policy applies to all Members, Committees, Employees of the Council, contractual third parties and agents of the Council who have access to Information Systems or information used for Ufford Parish Council purposes.

2) Information takes many forms and includes:

   - hard copy data printed or written on paper
   - data stored electronically
   - communications sent by post / courier or using electronic means
   - stored tape or video
   - speech

Information Storage

1) All electronic information will be stored on centralised facilities to allow regular backups to take place.

2) Information will not be held that breaches the Data Protection Act 1998 or DPA 2018 or formal notification and guidance issued by Ufford Parish Council. All personal identifiable information will be used in accordance with the Caldicott Principles (see Appendix 1).

3) Records management and retention policy will be followed.

4) Members should not be allowed to access information until the Clerk is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

5) Databases holding personal information will have a defined security and system management policy for the records and documentation.

6) This documentation will include a clear statement as to the use, or planned use of the personal information, which is cross-referenced to the Data Protection Notification.

7) Files which are listed by Ufford Parish Council as a potential security risk should not be stored on the network, except for in designated application storage areas. To facilitate this Ufford Parish Council will implement an electronic File security solution.

Disclosure of Information - Computer and Paper Based

1) The disclosure of personal information to other than authorised persons is forbidden. If there is suspicion of a Member or employee treating confidential Council information in a way that could be harmful to the Council or to the data subject, then it is be reported to the Data Control Officer (Clerk) who will take appropriate action.

2) Printed documents, containing personal data, should not be distributed without the express consent of the information owner, or by the Clerk in exceptional circumstances

3) Personal or sensitive documents are not to be left unattended and, when not in use, are to be locked away and accessed only by authorised persons.

4) Disposal methods for waste computer printed output and other media must be in accordance with Ufford Parish Council's disposal policy.

5) Distribution of information should be via the most secure method available.

Disclosure of Information – Telephone, Fax and E-mail

Where this involves the exchange of sensitive information then the following procedures will be applied.

Telephone calls:

1) Verify the identification of the caller before disclosing information. If in doubt, return their call using a known telephone number.

2) Ensure that you are authorised to disclose the information requested.

3) Ensure that the person is entitled to be given this information.

4) Ensure that the information you give is accurate and factual.

Disclosure of information by email:

1) Personal or sensitive information is immediately at risk once transmitted.

2) If an e-mail is sent to an IP address the email will be delivered through the public network and the message may be left at several locations on its journey and could be deliberately intercepted.

3) Email should not be used for sending personal or sensitive information unless technical measures are in place to keep the message secure.

4) The sender should be satisfied of the identity of the recipient, if in doubt the email should not be sent and alternative methods should be used.

5) No identifiable personal information should be included when sending on emails.

6) Any e-mail received by a Member, regarding Council business, should be immediately forwarded to the Clerk.

Sharing of Personal Information

1) Information relating to individuals shall not be shared with other authorities without the agreement of the Data Protection Officer.
2) Members and the Clerk should be aware of their responsibilities to be able to justify the sharing of information and to be able to maintain security when transferring information in person, by email, phone or post.

Adopted by the Parish Council at a meeting on: *19th June 2018*

Signed:

Mrs Judi Hallett	Cllr. Kathryn Jones
Clerk	Chairman

Appendix 1

The Caldicott Principles revised 2013 are:

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

In April 2013, Dame Fiona Caldicott reported on her second review of information governance, her report "Information: To Share Or Not To Share? The Information Governance Review", informally known as the Caldicott2 Review, introduced a new 7th Caldicott Principle.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality