Information Security Policy
And Procedures for the Use of Information Technology

Introduction

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 regulate the use of personal data[1]. Uffington Parish Council ('the Council') has adopted and implemented new information security policy and procedures / practices for the use of information technology (IT) equipment, in the conduct of Council business.

Policy

The Council is fully committed to compliance with the GDPR and the Data Protection Act 2018. All data will be processed in accordance with relevant legislation, in order to ensure the confidentiality of the personal information of Councillors, the general public, and any other contractors and individuals for whom it holds any personal data. All other information will be handled in accordance with good practice.

The objectives of the Council's Information Security Policy are to preserve and ensure:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority, need to know and permission to process it.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly to prevent unauthorised access or changes.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

All members of the Council must be aware of the risks of the unnecessary disclosure of personal information, either by use of e-mail or the insecure handling of Council paperwork.

Procedures

General

- Councillors are encouraged to use tablets or similar for meetings, to avoid the printing, and possible loss or disclosure of sensitive information, on paper.

- Council documents, e-mail addresses and any other information the loss of which could prejudice the personal data of Councillors, the general public, contractors and other role holders is to be securely deleted or destroyed if the material in question is not covered by one of the special categories adopted by the Council (See the Council's Privacy Notices). Any data that is not included in one of the special categories adopted by the Council (See the Council's Privacy Notices) should be securely deleted or destroyed immediately it is no longer required for the use(s) specified.

E-mail

- All councillors should use only an email address provided for the sole use of transmitting and receiving Council, and Council-related, emails. This address will be of the form firstname.lastname@uffington.net . Passwords to these accounts will be held securely by the Clerk.

- E-mails to multiple addressees should be on a bcc basis, to protect individual e-mail addresses, unless the distribution is restricted to Council members only.

- Any e-mail which includes a chain of earlier e-mails should be cut off after three e-mails (unless a longer thread is essential for maintaining the logic of a conversation) to avoid the risk of personal data being prejudiced by mistake.

[1] Personal data means any information relating to an identified or identifiable natural person. For a full definition see https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data-1-0.pdf

- Consent to process personal data will be sought from addresses on the distribution of group e-mails used by the Council in accordance with the Council's Privacy Notice(s).

- E-mail for Council business on personal devices should be backed up regularly.

IT Equipment

- Access to all IT equipment which contains personal data relevant to Council business (personal computers, laptops, tablets, smart phones etc) should be password protected and held within a locked building/room when unattended. On devices with multiple users, a separate account, accessible only by the councillor, should be maintained for Council business.

- All IT equipment which contains personal data relevant to the Council business (personal computers, laptops, tablets, smart phones etc) should have an up-to-date[2] operating system and anti-virus protection software installed. Any connection to a Wi-Fi network should only be made via a secure link; unsecured public hotspots should be avoided.

Data Backup

Maintaining backups of all business critical data is essential. Individual councillors are responsible for backing up the data they hold on personal devices and the same security and access controls should be afforded to backup copies of data as for working data. The Clerk is responsible for backing up all other Council data which should be carried out as follows:

- Data which is the property of the Council should be backed up separately from any other data held by the Clerk.

- Data should be backed up to 2 separate, encrypted, devices (eg a removable drive) alternately and at least monthly.

- One copy of the data back-up is to be retained at the Clerk's home office, with the second copy stored off site with either the Chairman or Vice Chairman. The two copies are to be rotated at least monthly.

- If a cloud solution is adopted, the 2rd copy will be stored with a UK based Cloud provider rather than with the Chairman or Vice Chairman.

Village website

Our website is provided by a third-party company (currently 1and1/Ionos). In accordance with industry norms, our provider collects standard internet log information and details of visitor behaviour patterns in order to monitor and report on such things such as:

- Visitor figures: Visitors, sessions, page impressions and search engine bots.
- Visitor behaviour: Average session duration, page impressions per session and bounce rate.
- Page analysis: Landing pages, exit pages, error pages, most visited pages, pages with high bounce rates and search terms.
- Origins: All pages of origin and referring pages.
- Browsers & systems: Browsers, browser versions, operating systems and operating system versions.
- More information on the 1and/Ionos Privacy policy can viewed here https://www.ionos.co.uk/terms-gtc/privacy-policy/

Website information is only processed by the website provider in a way which does not identify anyone.

[2] 'Up-to-date' in this context means an operating system which is still maintained with security updates by the manufacturer.

The website contains names and contact information for all councillors and a number of social and commercial services and facilities. By placing this data on the website, the owners of the data are agreeing for it to be in the public domain.

Use of Cookies. Our website uses only technical cookies; these are cookies used to provide for a smooth running website. For example, technical cookies help in collecting and storing items in online shopping carts. User consent is not required.

Disclosure of personal information. We collect contact and other information via the web site on a lawful basis for the purposes of providing a service to existing and potential visitors to our website. If we need to collect personally identifiable information through our website, we will be clear about this on any page from which the information is collected (eg the Contact Us page). We will make it clear when we collect personal information and will explain what we intend to do with it. We will never disclose personal details without the consent of the owner. Details are only held for as long as is necessary to fulfil the service request.

Links to other websites. Where we provide links to other websites outside our control, we will state that this is the case. Our privacy notice does not cover the links from within our site to other websites. We encourage you to read the privacy statements on the other websites you visit.

Action on Personal Data Breaches

A personal data breach can be broadly definedi as *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.*

In the event of becoming aware of such a breach any councillor is to report it to the Chairman and Clerk as soon as practicable using the form at Appendix 1 and, subject to the breach being confirmed, the following 4 step action plan is to be adopted:

1. Containment and Recovery. Take any immediate steps to prevent any further breach of the same data by suspending all but essential processing activity. A councillor should be nominated to work with the Clerk to carry out the next 3 steps.

2. Assessment and Ongoing Risk Assessment. The appointed councillor and Clerk are to conduct a risk analysis using a likelihood vs impact assessment. The Chairman will review the assessment and agree the risk level.

3. Notification of the Breach. Complete the ICO data breach notification form[3], submit only if it meets the ICO threshold of a "serious breach".

4. Evaluation and Response. It is important to investigate the causes of the breach and evaluate the effectiveness of the response. If the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing 'business as usual' is not acceptable. Similarly, if the response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update this policy and lines responsibility in the light of experience.

Appendix 1 – Data Breach Notification Form

Last updated: January 2020
Adopted by the Council on: -

[3] https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

APPENDIX 1

DATA BREACH REPORT FORM

Councillors must act promptly to report any data breaches. If you discover a data breach, please notify the Parish Chairman and Clerk immediately, complete Section 1 of this form and email it to the Parish Clerk (uffingtonpc.clerk@gmail.com)

Section 1: Notification of Data Security Breach	**To be completed by the person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: **Assessment of Severity and Ongoing Risk**	**To be completed by the appointed councilor in consultation with the Clerk.**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to vulnerable adults and children;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	
Clerk and nominated councilor to discuss with Chairman agree ongoing risk	

Section 3: Response and Notification	**To be completed by the Clerk**
Incident number	**e.g. year/00n**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to Clerk on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Clerk:	
Notification to ICO if breach exceeds the ICO 'Serious Breach' threshold (using ICO breach notification form)	**YES/NO If YES, notified on:** **Details:**
Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**

Section 4: Evaluation	**To be completed by the nominated councilor and Clerk**
Evaluation of the effectiveness of the response	**List all lessons identified**
Updated Policy (if necessary)	**Policy Updated: Yes/No** **Date:**