West Hendred Parish Council

Information Security Policy
And Procedures for the Use of Information Technology

Introduction

The requirements of the General Data Protection Regulation (GDPR) and a new Data Protection Act require West Hendred Parish Council ('the Council') to adopt and implement a 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 other data protection legislation. 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 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.

- 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.

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

IT Equipment

- Access to all IT equipment which contains personal data relevant to the Council (personal computers, lap tops, 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 (personal computers, lap tops, tablets, smart phones etc) should have up-to-date 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 a separate, encrypted, device (eg a removable drive) at least weekly.

- Backed up data should be stored off-site from the original data and held by another member of the Council.

Village website

Our website is provided by a third party company (currently 1and1). 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.

The website contains names, addresses and contact information for 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.

This information is only processed in a way which does not identify anyone. If we do want 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.

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 details via the web site for the purposes of providing a service to existing and potential visitors to our website. 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 within our site, linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

Last updated: June 2018.
Adopted by the Council on: 13th September 2018