HELLESDON PARISH COUNCIL

Information Security Policy

1. Policy Statement

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals personal data when it is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

Hellesdon Parish Council is dedicated to ensuring the protection of all information assets within the keeping of the Parish Council.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

The Parish Council will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information security policy within the Parish Council including the supporting guidance documents which are listed below.

This Policy sets out the measures taken by the Parish Council to achieve this,

including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support the Parish Council Data Protection Policy in ensuring all staff/committee members are aware of and comply with UK law and Parish Council procedures applying to the processing of data; and
- increase awareness and understanding at the Parish Council of the requirements of information security and the responsibility for staff/council members to protect the confidentiality and integrity of the information that they process.

2. Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

For the avoidance of doubt, the term ‘mobile devices’ used in this policy refers to any removable media or mobile device that stores data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

3. Purpose

Information is a major asset that the Parish Council has a responsibility and requirement to protect. The secure running of the Parish Council is dependent on information being held safely and securely.

Information used by the Parish Council exists in many forms and this policy includes the protection of information stored electronically, transmitted across networks and printed or written on paper. It also includes any information assets in Cyberspace (The Cloud). UK Cyber Security Strategy 2011 defined Cyberspace as:

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services".

Protecting personal information is a legal requirement under Data Protection Law. The Parish Council must ensure that it can provide appropriate assurances to its residents and staff/committee members about the way that it looks after information ensuring that their privacy is protected, and their personal information is handled professionally.

Protecting information assets is not simply limited to covering the information (electronic data or paper records) that the Parish Council maintains, it also addresses who has access to that information, the processes they follow, and the physical computer equipment used to access them.

This policy details the basic requirements and responsibilities for the proper management of information assets.

4. Scope

This Information Security Policy applies to all systems, written, spoken and electronic information held, used or transmitted by or on behalf of the Parish Council, in whatever media.

This includes information held on computer systems, paper records, hand-held devices and information transmitted orally.

This policy applies to all members of staff/members/committee members, including temporary workers, contractors, volunteers and any and all third parties authorised to use the IT systems. All staff and members are required to familiarise themselves with its content and comply with provisions contained in it. Breach of this policy by staff can be treated as a disciplinary offence which may result in disciplinary action under the Parish Council's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach. Breach of this policy by members will be deemed as an infringement of the Members' Code of Conduct and can result in a report to the monitoring officer.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations and processes that make up the Parish Council's information systems. This includes all Parish Council staff and members.

5. General Principles

All data stored on Parish Council IT Systems or paper records shall be available only to staff or members with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All Parish Council owned IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the Parish Council's IT Consultant or by such third party/parties as the Parish Council may authorise.

All staff/committee members have an obligation to report actual and potential data protection compliance failures to the Parish Council Clerk who acts as Data Protection Officer who shall investigate the breach.

6. Risks

The Parish Council recognises that there are risks associated with users accessing and handling information in order to conduct official Parish Council business.

The Parish Council is committed to maintaining and improving information security and minimising its exposure to risks. It is the policy of the Parish Council to use all reasonable, practical and cost-effective measures to ensure that:

- Information will be protected against unauthorised access and disclosure
- The confidentiality of information will be assured
- The integrity and quality of information will be maintained
- Authorised staff, when required, will have access to relevant Parish Council systems and information.
- The Parish Council systems have a contingency in place for business continuity and disaster recovery.
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/ documented agreements.
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be available to staff/committee members on request.

Non-compliance with this policy could have a significant effect on the efficient operation of the Parish Council and may result in financial loss and embarrassment.

7. Physical Security and Procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked filing cabinets and locked cupboards shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office desks, on meeting tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of Parish Council owned buildings.

If you find the security to be insufficient, you must inform the Clerk and Responsible Officer as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The Parish Council carried out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.

The Parish Council secures the buildings at certain times to prevent unauthorised access to the buildings. An alarm system is set nightly. CCTV Cameras are in use at the Parish Council and monitored by Staff.

Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

8. Roles and Responsibilities

It is the responsibility of each member of staff and council member to adhere to this policy, standards and procedures. It is the Parish Council's responsibility to ensure the security of their information, ICT assets and data. All members of the Parish Council have a role to play in information security.

The Clerk and Responsible Officer in conjunction with councillors and IT consultant shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Parish Council's security requirements;

b) ensuring that IT Security standards within the Parish Council are effectively implemented and regularly reviewed, working in consultation with the Parish Council's management, and reporting the outcome of such reviews to the Parish Council's management;
c) ensuring that all members of staff and council members are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990. Furthermore, the IT Consultant, in conjunction with the Clerk and Responsible Officer and councillors shall be responsible for the following:

- assisting all members of staff/councillors in understanding and complying with this policy;
- providing all members of staff/councillors with appropriate support and training in IT Security matters and use of IT Systems;
- ensuring that all members of staff/councillors are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
- receiving and handling all reports relating to IT Security matters and taking appropriate action in response.
- taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff/councillors;
- monitoring all IT security within the Parish Council and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

9. All Staff/councillors

All members of staff/councillors must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

Staff/councillors must immediately inform the Clerk and Responsible Officer of any and all security concerns relating to the IT Systems which could or has led to a data breach.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the Clerk and Responsible Officer immediately.

You are not entitled to install any software of your own without the approval of the Parish Council's IT Consultant.

Physical media (e.g. USB memory sticks or disks of any kind) should not be used for

transferring files without permission.

If you detect any virus this must be reported immediately to the Parish Council's IT Consultant (this rule shall apply even where the anti-virus software automatically fixes the problem).

10. Access Security

All members of staff/councillors are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The Parish Council has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Parish Council's network.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode. All passwords must, where the software, computer, or device allows:

a) be at least 6 characters long including numbers, letters and a special character (eg: $%£);
b) be changed on a regular basis;
c) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Clerk and Responsible Officer who will liaise with the IT Consultant as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation may be liable to disciplinary action under the Parish Council's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password may be liable to disciplinary action up to and including summary dismissal for gross misconduct. Councillors who have been found to have committed a similar offence will be liable to be reported to the monitoring officer under the Members' Code of Conduct.

If you forget your password, you should notify the Parish Council's IT Consultant to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If you must write down passwords ensure that you store them securely (e.g. in a locked drawer or in a secure password database).

Passwords should never be left on display for others to see. Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the Parish Council, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff members should be aware that if they fail to log off and leave their terminals unattended, they may be held responsible for another user's activities on their terminal in breach of this policy, the Parish Council's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

11. Data Security

Personal data sent over the Parish Council network will be encrypted or otherwise secured. All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Parish Council's IT Consultant who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the Parish Council's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the Parish Council's Wi-Fi. All usage of your own device(s) whilst connected to the Parish Council's network or any other part of the IT Systems is subject to all relevant Parish Council Policies (including, but not limited to, this policy). The Clerk and Responsible Officer and/or the Parish Council's IT Consultant may at any time request the immediate disconnection of any such devices without notice.

12. Electronic Storage of Data

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the IT Consultant. No data to be stored electronically on physical media. You should not store any personal data on any mobile device, whether such device belongs to the Parish Council. Data may only be stored on the Parish Council's computer network in order for it to be backed up. All electronic data must be securely backed up by the end of the each working day and is done by Automated Processing.

13. Home Working

You should not take confidential or other information home without prior permission of the Clerk and Responsible Officer, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
b) all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.

14. Communications, Transfer, Internet and Email Use

The Parish Council works to ensure the systems do protect residents and staff/councillors and are reviewed and improved regularly.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee, and the Parish Council cannot accept liability for the material accessed or its consequence.

Postal and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the Parish Council.

Personal or confidential information should not be removed from the Parish Council without prior permission from the Clerk and Responsible Officer. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained.

You must ensure that the information is:

- not transported in see-through or other un-secured bags or cases;
- not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- not left unattended or in any place where it is at risk (e.g.in car boots, cafes, etc.)

15. Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Clerk and Responsible Officer. All members of staff/councillors have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Clerk and Responsible Officer shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff/councillors shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Clerk and Responsible Officer, who may then pass on the matter to the Parish Council's IT Consultant.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Clerk and Responsible Officer.

All IT security breaches shall be fully documented.

16. Types of security incidents

A data security breach can happen for many reasons:

- Loss or theft of data or equipment on which data is stored i.e. IT equipment or information (laptops, mobiles, devices containing personal data e.g. memory sticks)
- Unauthorised disclosure containing personal information
- Inappropriate access controls allowing unauthorised use
- Breach of physical building access/security
- Human error e.g. personal information being left in an insecure location, using incorrect email or postal address, uploading personal information to a website
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deception

17. Reporting a security incident

This section explains how to report a security incident including a data breach.

- The person who discovered the security incident MUST report the security incident to the Clerk and Responsible Officer immediately and no later than 24 hours after the incident. If this is not possible then the Chair should be informed. If the incident occurs or is discovered outside normal working hours this should be done as soon as practicable.
- The Clerk and Responsible Officer will determine and lead on an investigation although others may be invited to assist depending on the severity of the security incident. Staff must not attempt to conduct their own investigations (other than reporting the incident).
- Any decision to take disciplinary action will be in line with the Parish Council's disciplinary policy.
- The security incident report will be concluded when all investigations are complete.

18. Responsibility of Clerk and Responsible Officer Breach Management Plan
The Clerk and Responsible Officer will lead all data breach investigations and will follow the Information Commissioner's Office (ICO) suggested Breach Management Plan:-

1. Containment and Recovery

2. Assessment of ongoing risk

3. Notification of Breach

4. Evaluation and Response

Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data breach including, where necessary, damage limitation. The Clerk and Responsible Person will:

- Lead the investigation , drawing on the expertise of the Parish Council's IT Consultant if required.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a process, finding a lost piece of equipment, or simply changing access codes etc.
- Establish if there is anything that can be done to recover any losses and limit the damage the breach can cause.
- Where appropriate inform the ICO within 24 - 72 hours and;
- Where appropriate inform the police

Assessing the risks

The next stage of the management plan is for the Clerk and Responsible Officer to assess the risks which may be associated with the breach considering the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. In making this assessment the Clerk and Responsible Officer will assess:

- What type of data is involved
- How sensitive it is
- If data has been lost or stolen are there any protections in place such as encryption
- What has happened to the data
- What are the consequences if a third party has the data
- How many and who are the individuals' affected
- What harm can come to those individuals

- If there are wider consequences to consider such as a risk to public health or loss of public confidence

Notification

The Clerk and Responsible Officer will decide whether the Information Commissioner's Office (ICO) or the data subjects should be notified of the breach and will inform the Chair. The ICO must be notified within 24 – 72 hours.

The ICO will need to be notified of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals, for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This will be assessed on a case by case basis by the Clerk and Responsible Officer.

Evaluation and Response

The Clerk and Responsible Officer will:

- fully review both the causes of the breach and the effectiveness of the response to it
- keep a breach log
- report to the Chair and full council
- implement an action plan to correct identified issues if required
- monitor staff awareness of security issues and look to fill any gaps through training