Controlled Document

Title	Information Security Policy
Author	Lenham Parish Council
Owner	Lenham Parish Council
Subject	Main Policy Documents
Government Security Classification	Official
Document Version	Version 1
Created	29.08.25
Approved By	Full Council
Review Date	September 2027

Version Control

Version	Date	Author	Description of Change	Sign/Date
1	**01.10.25**	**Lenham Parish Council**	**Original Policy**	**L.Westcott**

Information Security Policy

Policy Statement

The General Data Protection Regulation (UK 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.

Lenham Parish Council (hereinafter referred to as the '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 always maintained.

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:-

a. Protect against potential breaches of confidentiality,
b. Ensure that all information assets and IT facilities are protected against damage, loss or misuse,
c. 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
d. Increase awareness and understanding at the Parish Council of the requirements of information security and the responsibility for staff/ committee members to protect the confidentiality and integrity of the information that they process.

Purpose

This policy applies to all members of staff, including temporary workers, council member, contractors, volunteers and all third parties authorise to use the IT systems. All of these groups are required to familiarise themselves with its contents and comply with provisions contained in it.

Information security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. 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 the networks and printed or written on paper. It also includes any information assets in Cyberspace (The Cloud). Uk Cyber Security Strategy 2011 defines Cyberspace as:

"*Cyberspace is an interaction email made up of digital networks that issued to store, modify and communicate information. It includes the internet, but also the other information systems that support out businesses, infrastructure and service*".

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.

Scope

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

This Information Security Policy apply 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.

Breach of this policy will 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.

This policy does not form part of any individual's terms and conditions of employment with the Parish Council and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy to remain compliant with legal obligations and processes that make up the Parish Council's information systems. This includes all Parish Council staff, council members and agents of the Parish Council who have access to Information Systems or information used for Parish Council purposes.

General Principles

All data stored on Parish Council IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information).
All data classified must be handled appropriately in accordance with its classification.

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

All IT systems are to be installed, maintained, serviced, repaired and upgraded by IT Consultant or by such third party/parties as the Chair and Committee members may authorise.

The responsibility for the security and integrity of all IT systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Chair and Committee members unless expressly stated otherwise.

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

Risks

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

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

a. Information will be protected against unauthorised access and disclosure,
b. The confidentiality of information will be assured,
c. The integrity and quality of information will be maintained,
d. Authorised staff/ committee members, when required, will have access to relevant Parish Council systems and information,
e. Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained,
f. Access to information and information processing facilities by third partes will be strictly controlled with detailed responsibilities written into contract/ documentation agreement.
g. All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
h. 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.

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 this is general access unless there is a legal reason to be given and/ or relevant consents have been obtained. You should take particular care if documents must be taken out of Parish Council owned buildings.

The physical security of buildings and storage systems should be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Clerk as soon as possible. Increased risks of vandalism and burglary should be considered when assessing the level of security required.

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

The Parish Council secure the buildings at certain times to prevent unauthorised access to the buildings. An alarm is set nightly.

CCTV cameras are in use at the Parish Council office and monitored by staff.

Visitors should be required to sign the visitors' book and never left along in areas when they could access confidential information.

Roles and Responsibilities

It is the responsibility of each member of staff/ committee 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 in conjunction with councillors and IT consultants shall be responsible for the following:

- Ensuring that all IT systems are assessed and deemed suitable for compliance with the Parish Council's security requirements;
- Ensuring that IT security standards with 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 management;
- Ensuring that all members of staff/committee 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 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.
- Ensure that all members of staff/councillors are granted levels of access to IT systems that are appropriate for each member, considering 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 including, if any reports relating to personal data, informing the Clerk;

- 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 off all data stored within the IT systems at regular intervals and that such backups are stored at a suitable location offsite.
- All members of staff/councillors must always comply with all relevant parts of this policy when using the IT systems.
- Computers and other electronic devices should be locked when not in use to minimise accidental loss or disclosure.
- Staff/Councillors must immediately inform the Clerk of all data security concerns relating to the IT system which could or has led to a data breach as set out in the Breach Notification Policy.
- Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT systems should be reported to the Clerk immediately.

You are not entitled to install any software of your own without the approval of the Clerk. Any software belonging to you must be approved by the Clerk and may only be installed where that installation poses no security risk to the IT system and where the installation would not breach any license agreements to which that software may be subject. Prior to installation of any software onto the IT systems you must obtain written permission from the Clerk and RFO. This permission must clearly state which software you may install, and onto which computer (s) or device (S) may be installed.

Physical media (e.g. USB memory sticks or disks of any kind) may not be used for transferring files outside of the office. The Clerk's approval must be obtained prior to transferring files using cloud storage systems.

If you detect any virus this must be reported immediately to the Clerk (this rule shall apply even when the anti-virus software automatically fixes the problem.

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 the policy.

The Parish Council has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and protect the Parish Council's network. The Parish Council also provides training to ensure everyone is aware of how to protect the Parish Council's network and themselves.

All IT Systems (mobile devices) should be protected with a secure password or passcode or other form of secure log-in system as approved by the Clerk. Biometric log-in methods can only be used if approved by the Clerk.

All passwords must be used, where the software, computer, or devices allow:

- Be at least 6 characters long including numbers, letters and a special character (e.g. %$£&);
- Be changed on a regular basis.
- Not to be obvious or easily guessed (e.g birthday 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 who will liaise with the IT Consultant as appropriate and necessary. Any member of staff/councillor who discloses his or her password to another employee/councillor in the absence of express authorisation will be liable to disciplinary action under the Parish Council Disciplinary Policy and Procedure. Any member of staff/committee member who logs onto a computer system using another member of staff/committee members password will be liable to disciplinary action.

If you forgot your password, you should notify the Clerk 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 never write down passwords if it is possible to remember them. If you must write them down, ensure 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 (i.e. mouse, keyboards, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change 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.

Staff/council 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.

Data Security

Personal data sent over Parish Council network will be encrypted or otherwise secured.
All members of staff/councillors are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Clerk 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 unknow origins. Where consent is given all files and data should be virus checked before they are downloaded onto the Parish Council's system.

You may connect your own devices (including, but not limited to laptops, tablets, and smartphones) to the Parish Council's wi-fi provided that you follow the Parish Council's

requirements and instructions governing this use. All usage of your own device(s) whilst connected to the Parish Council's network or any other part of the IT system is subject to all relevant Parish Council Policies (including but not limited to this policy). The Clerk may at anytime request the immediate disconnection of any such devices without notice.

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 should be stored electronically on physical media.

You should not store any personal data on any mobile device, whether such devices belong to the Parish Council.

Data may only be stored on the Parish Council's computer network for it to be backed up.
All electronic data must be securely backed up by the end of each working day and is done by Automated Processing.

Home Working

You should not take confidential or other information home without prior permission of the Clerk 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:

- The information is kept in a secure and locked environment where it cannot be accessed by a family member or visitor; and
- All confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.
- When using the Parish Councils IT systems, you are subject to and must comply with the Parish Council Acceptable User policy.
- The Parish Council work to ensure the systems protect residents and staff/councillors and are reviewed and improved regularly.
- If staff/councillors or residents discover unsuitable sites or any material which would be unsuitable, this should be reported to the Clerk.
- 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 consequences.
- All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email or sent by tracked DX (document exchange) or recorded delivery.
- Postal, DX and email addresses and numbers should be checked and verified before you send information to them. 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 except where the removal is temporary and necessary. 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 please (e.g waiting room, cafes, trains etc.) and
- Not left unattended or in any place where it is at risk (e.g. car boot, café etc.)

Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Clerk. 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 shall immediately access the issue, including but not limited to the level of risk associated with the issue, and shall take all the steps necessary to respond to the issue.

Members of staff/ councillors shall under no circumstances attempt to resolve an IT breach on their own without first consulting the Clerk. Any attempt to resolve an IT security breach by a member of staff/councillor must be under the instruction of, and with the express permission of the Clerk.

All IT security breaches shall be fully documented.

Full details on how to notify of a data breach are set out in the Security Incident and Data Breach Notification Policy.

Policy Review

The Clerk is responsible for monitoring and reviewing this policy. This policy will be reviewed every 2 years. In addition, changes to legislation, national guidance, codes of practice or commissioners' advice may trigger interim reviews.