STAPLEHURST PARISH COUNCIL

IT Policy

1. Introduction

1.1. This policy has been adopted by the Parish Council ("Council") in order to:

1.1.1. prevent inappropriate use of computer equipment (such as extended personal use or for accessing and circulating pornographic, racist, sexist or defamatory material).

1.1.2. protect confidential, personal or commercially sensitive data.

1.1.3. prevent the introduction of viruses.

1.1.4. prevent the use of unlicensed software.

1.1.5. ensure that Council property is properly looked after.

1.1.6. monitor the use of computer IT facilities to ensure compliance with internal policies and rules and to detect abuse.

1.2. The consequences of misuse can be severe. Examples of potential damage include, but are not limited to, malware infections, legal and financial penalties for data leakage and lost productivity from network downtime.

1.3. The Council provides Councillors and employees with access to various computing and telephone communication methods ("IT facilities") to allow them to undertake the responsibilities of their position and to improve internal and external communication.

1.4. This policy supports the Councils adopted Communications Strategy.

2. Legislative Context

- This policy is informed by the following legislation and guidance:
- UK General Data Protection Regulation (UK GDPR)

- Data Protection Act 2018
- Freedom of Information Act 2000
- Local Government Act 1972
- NALC Legal Topic Notes (especially LTN 40: Councillor communications)
- The Seven Principles of Public Life (Nolan Principles)

3. Scope

3.1. This policy sets out the Council's position on the use of the IT facilities and it includes:

3.1.1. Employees and Councillors' responsibilities and potential liability when using the IT facilities.

3.1.2. the monitoring policies adopted by the Council; and guidance on how to use the IT facilities.

3.2. This policy has been created to:

3.2.1. ensure compliance with all applicable laws relating to data protection, information security and compliance monitoring

3.2.2. protect the Council from the risk of financial loss, loss of reputation or libel

3.2.3. ensure that the IT facilities are not used so as to cause harm or damage to any person or organisation.

3.3. This policy applies to the use of:

3.3.1. local, inter-office, national and international, private or public networks and all systems and services accessed through those networks.

3.3.2. desktop, portable, mobile phones and mobile computers and applications owned or leased by the Council.

3.3.3. electronic mail and messaging services.

4. Breach of the Policy

4.1. In respect of employees, breach of this policy will be regarded as a disciplinary offence and will be dealt with under the Council's disciplinary process.

4.2. In respect of Councillors, breach of Policy will be reported to the Monitoring Officer.

4.3. Anyone who considers that there has been a breach of this policy in relation to personal information about them held by the Council should raise the matter via the Council's formal GDPR procedure.

5. Email (Internal or External Use)

5.1. All Councillors and relevant employees will be issued with a Council email account which must always be used when transacting on behalf of the Parish Council. Such an account will only be used for Council correspondence.

5.2. Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should either be sent using password protected attachments or by using a password protected link to documents in SharePoint.

5.3. Email should be treated as any other documentation. If you would normally retain a certain document in hard copy, you should retain the email.

5.4. Do not forward email messages unless the original sender is aware that the message may be forwarded and that the whole email chain has been checked for appropriate content. If you would not have forwarded a copy of a paper memo with the same information **do not** forward the email.

5.5. It is good practice to copy and paste information from an email to pass it on, rather than forwarding on an email, in order to remove the previous email address from the header.

5.6. Personal emails are subject to Freedom of Information requests/subject access requests, if they relate to Council business or an individual and it is a criminal offence to block the release of data.

5.7. Council emails should not be forwarded to a personal account without the Data Controller's permission and doing so is a breach of the Data Protection Act and Computer Misuse Act.

5.8. Your email inbox should be checked for new emails on a regular basis.

5.9. As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

5.10. Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of an email account is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

5.11. Councillors and employees will be required to surrender their email account and all of its contents to the Clerk when they leave the Council. The Clerk on leaving the Council needs to do the same, but to the Chair of the Parish Council.

6. Use of Laptop computers, PC's, tablets and smart phones

The Council has adopted Microsoft Office 365; this means that Councillors as well as employee can work collaborative in the Councils IT filing system. This has many advantages but also carries risk of security**.**

IT equipment belonging to the Council and used by Councillors

6.1. Laptop computers, PC's, tablets and smart phones belonging to the Council along with related equipment and software are subject to all of the Council's policies and guidelines governing non-portable computers and software. All laptops, PC's and tablets will be encrypted.

6.2. When using such equipment:

6.2.1. You are responsible for all equipment and software until you return it. It must be kept secure at all times.

6.2.2. The Clerk and the individual employees or Councillor are the only persons authorised to use the equipment and software issued to that employee or Councillor.

6.2.3. Every employee or Councillor must work within the Councils filing/software environment when carrying out Council business to ensure that all data is backed up and accessible by the Clerk.

6.2.4. If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the Council's attention, initially through the Clerk or in their absence, the Deputy Clerk.

6.2.5. Upon the request of the Council at any time, for any reason, you will immediately return any equipment and all software to the

Council.

6.2.6. Software piracy could expose both the Council and the user to allegations of intellectual property infringement. The Council is committed to following the terms of all software licenses to which the Council is a contracting party. This means, that:

6.2.6.1. software must not be installed onto any of the Council's computers unless this has been approved in advance by our IT Contractors or Council. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus-free and compatible with the computer IT facilities.

6.2.6.2. software should not be removed from any computer, nor should it be copied or loaded on to any computer without prior consent.

6.2.7. In order to maintain the confidentiality of information held on or transferred via the Council's equipment, security measures are in place and must be followed at all times. A log-on ID and password are required for access to the Council's equipment/network. This will be changed regularly and must be kept secure and not shared with anyone. If Cllrs or employees forget their log on ID / passwords the Council's IT service provider can reset them with a temporary password, which the Councillor's can reset.

6.2.8. You are expressly prohibited from using the equipment for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Council or its clients other than in the normal and proper course of carrying out your duties for the Council.

6.2.9. In order to ensure proper use of Council computers, you must adhere to the following practices:

6.2.9.1. anti-virus software must be kept running at all times.

6.2.9.2. media storage such as USB drives, CD's or portable hard drives will **not** be permitted unless they have been provided by the IT contractor or approved by Council.

6.2.9.3. obvious passwords such as birthdays and spouse names, etc, must be avoided (the most secure passwords are random combinations of letters and numbers).

6.2.9.4. all files are stored on the Council's cloud drive which is backed up regularly to avoid loss of information.

6.2.9.5. always log off the computer/network before leaving your computer for long periods of time or overnight.

6.2.9.6. Council owned IT equipment is covered by Council Insurance.

6.3 Councillor's and employees using Council equipment should sign the Disclaimer attached in **Appendix A.**

Councillor's using their own IT equipment for Council work.

6.4 Councillors and employees using their own personal equipment should adhere to 6.1 to 6.3 of this policy, however Councillors and employees using their own equipment are not insured by the Council. and sign the Declaration attached in **Appendix B**.

7. Internet

7.1. Refer to the Council's adopted Communications Policy on the use of social media.

7.2. Employees and Councillors using their own social media accounts must ensure that any comment made is clearly identified as their own and **not** representative of the Parish Council.

7.3. Using the internet for the purpose of trading or carrying out any business activity other than Council business is strictly prohibited.

7.4. For the avoidance of doubt the matters set out above include use of Council wireless IT facilities.

8. Monitoring Policy

8.1. The policy of the Council is that we may monitor your use of the equipment.

8.2. The Council recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the equipment.

8.3. The Council may from time to time monitor the equipment. The principal reasons for this are to:

8.3.1. detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex

discrimination policies.

8.3.2. ensure compliance with this policy.

8.3.3. detect and enforce the integrity of the equipment and any sensitive or confidential information belonging to or under the control of the Council.

8.3.4. ensure compliance by users of the equipment with all applicable laws (including data protection), regulations and guidelines published and in force from time to time.

8.3.5. monitor and protect the wellbeing of employees and Councillors.

8.4. The Council may adopt at any time a number of methods to monitor the use of the IT facilities. These may include:

8.4.1. recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content.

8.4.2. recording and logging the activities by individual users of the IT facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the internet and websites visited.

8.4.3. physical inspections of individual users' computers, software and telephone messaging services.

8.4.4. periodic monitoring of the IT facilities through third party software including real time inspections.

8.4.5. physical inspection of an individual's post.

8.4.6. archiving any information obtained from the above including emails, telephone call logs and Internet downloads.

8.5. The Council will not (unless required by law):

8.5.1. allow third parties to monitor the IT facilities (with the exception of our appointed IT contractor); or

8.5.2. disclose information obtained by such monitoring of the IT facilities to third parties unless the law permits.

8.6. The Council may be prohibited by law from notifying employees using the equipment of a disclosure to third parties.

9. General guidance

9.1. Never leave any equipment or data (including client files, laptops, computer equipment and mobile phones) unattended on public transport or in an unattended vehicle.

9.2. Observation of this policy is mandatory and forms part of the terms and conditions of employment of employees and the terms of access to the Council's systems and offices. Misuse of the IT facilities will be treated as gross misconduct and may lead to dismissal.

9.3. Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be taken with these devices: sensitive information should be stored in password protected or encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

9.4. All workstations (desktops and laptops) must be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

9.5. The downloading of documents onto IT equipment is prohibited as all work should be completed and stored in the Council's cloud software only.

10. Risks

10.1. The Council has identified the following risks inherent in using personally owned Devices to conduct Council Business:

Event / Action	Risk
Inadequate or lack of appropriate security measures used to control access to Device	Personal Data may be accessible to third parties
Device used in an insecure manner	Device could be affected by malware which could result in Personal Data being accessed by third parties

Device lost or stolen	Personal Data may be accessible to third parties
Device sold or given away	Personal Data may be accessible to third parties unless Device appropriately cleared before transfer by restoring factory settings
Employees cease to be employed by the Council or Councillor ceases to be a member of the Council	Personal Data may remain accessible via the Device and could be used for unauthorised purposes or disclosed to third parties

9.2 To mitigate the risk the Council will provide laptops for use by Councillors and employees. The only personal device to be used is smartphones for emails.

11. Leaving the Parish Council

11.1. If a Councillor ceases to be a member of the Council for any reason:

11.1.1. Councillors must return Devices issued by the Council immediately to the Clerk

11.1.2. all Personal Data or other information received in the course of Council Business must be permanently deleted from personally owned Devices.

11.1.3. all hard copies should be shredded or passed to the Clerk for destruction

11.2. On the termination of employees' employment by the Council:

11.2.1. employees must return Devices issued by the Council immediately; and

11.2.2. all Personal Data or other information received in the course of Council Business must be permanently deleted from personally owned Devices.

11.2.3. all hard copies should be shredded or passed to the Clerk for destruction

This Policy supersedes any former Parish Council IT Policy and was adopted by Staplehurst Parish Council on …26th August 2025……..Minute number 2388/6.5…….

Appendix A

Councillor IT equipment disclaimer - Use of SPC owned equipment

I ……..…….
have read and understand Staplehurst Parish Council's IT Policy and this disclaimer document allows me to use Staplehurst Parish Council (SPC) owned IT equipment for SPC business only.

The IT Equipment is ……..…….....

S/N: ……..…

1. I agree to use the SPC owned equipment named above for SPC business only.

2. I agree to keep the equipment password protected, and to not share this password with anyone unauthorised.

3. I agree to ensure that the security and antivirus software will be kept up to date (i.e. allowing updates when requested)

4. I agree that I am the responsible keeper of the IT equipment named above, and understand that the equipment is owned by SPC

5. I agree that I will allow the IT Contractor (Namely Heliocentrix) to have virtual access to the machine to access SPC business.

6. Freedom of Information Requests – From time to time the Council receives requests for Freedom of Information. Legally the Council must respond and therefore reserves the right to request any information on my Parish Council account.

7. Subject Access Review Requests; – From time to time the Council receives Subject Access Review Requests. Legally the Council must respond and therefore reserves the right to request any information on my Parish Council account.

Councillor

Print name…….…….

Signed……...Date……

Officer of Staplehurst Parish Council

Print name……..……

Signed……Date……

Appendix B

Councillor IT equipment disclaimer

I ……..…….
have read and understand Staplehurst Parish Council's (SPC) IT Policy and this disclaimer document allows me to use my own IT equipment for SPC business.

My IT Equipment is ……..……..

S/N: ……..…

1. I agree to only use the SPC owned software package accounts, including Microsoft365, Embedded apps (Outlook, Word etc.), OneDrive & Secure cloud servers, for SPC business.

#This does not mean that you cannot use 365 using another account, only that you cannot use your SPC account for any other business. #

2. I agree to not share my SPC login details with anyone

2a. I agree to not allow anyone unauthorized to use the SPC owned equipment #N/A to everyone, only those with SPC equipment #

3. I will keep security and antivirus up to date on my IT equipment #this means ensuring the software is kept up to date, our package has been built in protection#
4. I Understand that I am responsible for the maintenance of the hardware of my equipment.
5. I agree to allow the IT service contractor (Namely Heliocentrix) remote access to my SPC account if necessary
6. Freedom of Information Requests – From time to time the Council receives requests for Freedom of Information. Legally the Council must respond and therefore reserves the right to request any information on my Parish Council account.
7. Subject Access Review Requests; – From time to time the Council receives Subject Access Review Requests. Legally the Council must respond and therefore reserves the right to request any information on my Parish Council account. ## = Notes, will not be published

Councillor

Print name……

Signed……...……...Date…….

Officer of Staplehurst Parish Council

Print name……

Signed……..……...……...Date……