GORING-ON-THAMES PARISH COUNCIL

Goring-on-Thames Parish Council Information Technology Policy

---

This policy is written for everyone who makes use of computer equipment or services provided by the Council. This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It explains how everyone should conduct the Council's business in a secure and legal way when using IT equipment and software. The policy applies to the use of both council-owned equipment and also personal equipment for council business. It also outlines how and why the Council may monitor the use of these systems, and the likely consequences for anyone who breaches the policy.

It is expected that all councillors and staff should read this document carefully so that they are aware of the risks of using IT in general, and standards of conduct that are required in using IT in local government in particular.

If any councillor or member feels that any of the provisions of this policy might prevent them from doing Council business efficiently, they should discuss the problem with the Clerk, who may agree to specific and time-limited exemptions as appropriate.

The world of IT is constantly changing, so this policy cannot pretend to complete coverage, but no-one will go far wrong if they bear in mind the Nolan principles of public life and apply the same standards of selflessness, honesty, integrity, and openness to their use of IT as to any other aspect of their work. They should remain objective, hold themselves fully accountable for what they do, and actively promote proper use of the Council's systems at all times.

In this document "the Council" means Goring-on-Thames Parish Council.

This document assigns several roles and responsibilities to "the Clerk" – in all cases the responsibility remains with the Clerk, but the performance of the roles may be delegated as appropriate.

This document is an official policy of Goring-on-Thames Parish Council. It was written in January – February 2026, and adopted by the Council at a meeting in March 2026.

Signed: , Chair of the Council. Date:

GORING-ON-THAMES PARISH COUNCIL

Contents

1 Provision of IT equipment and systems for Council business

1.1 The Council provides and manages a range of IT systems that allow it to carry out its function as the first tier of local government in Goring. These systems include: the website that provides public information about the Council and its business; the email service for members of staff and councillors; standard office systems for documents and spreadsheets; payroll and accounting software to manage its finances; the burial ground management system; and mapping software to help manage assets around the village.

1.2 The Council does not operate public transactional services such as online payments or public user accounts, but may hold financial information relating to payments, reimbursements, grants, or other transactions as required for accounting and audit purposes.

1.3 The Council provides laptop computers for members of staff to allow them to use the systems to conduct Council business. The Council also provides mobile phones with a data contract for members of staff. Members of staff should never use personal equipment to conduct Council business.

1.4 In contrast the Council does not usually provide mobile phones or computer equipment for councillors. Councillors are expected to provide their own equipment to work with Council documents and spreadsheets and to access the Council email system; councillors do not usually access any other Council systems.

1.5 Lest this expectation discourage anyone from standing to be elected as a Councillor, an appropriately-configured computing device may be provided to an elected Councillor, at the discretion of the Clerk, after discussion with Chair of the Council, to enable them to use the Council systems.

1.6 All of the Council's business must be conducted according to the Nolan principles of openness and accountability. All of the Council's records, all written correspondence, all electronic correspondence, all policy documents, all minutes of Council meetings and committee meetings, and even hand-written records (excepting only rough working drafts) are required to be available for audit purposes and may be required to respond to a formal Freedom of Information request.

1.7 The Council therefore may require access at any time to Council-provided IT equipment. The Council may also request access to personal IT equipment being used for Council business and councillors should respond promptly and positively to any such requests, provided that there is a clearly-documented legal requirement.

1.8 The Council also has the right to monitor the use of IT equipment and systems that it has provided for Council business. The Council will not deploy any monitoring tools without first informing councillors, employees, and any other authorized users that the monitoring may take place, and explaining the legitimate reason for doing it. Any monitoring will be proportionate and will comply with relevant data-protection and privacy laws.

1.9 All users engaged in Council business are expected to use all systems in an ethical and respectful manner and in accordance with this policy. Irrespective of the ownership of the device used, accessing inappropriate websites or services via IT infrastructure provided by the Council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). For Workers or Contractors, the Council may terminate the worker agreement.

2 Use of Council-provided hardware and systems on Council premises

2.1 In the Council's office, the Council provides a local area network with a broad-band connection, a shared colour laser printer, and a ceiling-mounted overhead projector.

2.2 The council may also provide display screens, as well as computer keyboards and pointing devices, for members of staff who require them.

2.3 All computer equipment in the office should be treated with good care at all times. Each device should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto any of them. Any damage must be reported to the Clerk.

2.4 The maintenance of computer equipment in the office is the responsibility of the Clerk. No staff or councillors should attempt any form of maintenance of any equipment unless they have appropriate qualifications and they have agreed any work with the Clerk before it is started. If in doubt, the Clerk should engage a qualified professional.

Use of the network

2.5 The network consists of a network router device that connects to the Internet and provides four Ethernet ports and a WiFi service. One of the Ethernet ports is connected to the office printer, the others are usually left free. The router is configured to provide two separate WiFi network names: the private network name is for use of employees and councillors; the public network name is for the use of visitors and members of the public while they are in the office.

2.6 Each network name is secured with a password. The password for the public network may be advertised in the public meeting area. The password for the private network name may only be shared with employees and councillors. Both passwords should be changed at least every 12 months. The reason for providing two names is so that the networks may be configured differently; for example the public network may be scheduled to be turned off on certain days.

2.7 The connection to the Internet is provided for Council business use, such as accessing the Council email system, using the web to find the latest copy of the NALC Good Councillor guide, or reading the details of a planning application on the district council website. Limited personal use is also permitted. So an employee or a councilor might check for messages or emails from family members, or look up train times; or a visiting supplier might check product details on their company website.

2.8 The internet connection must not be used to disrupt council business or bring the Council into disrepute. Specifically prohibited activities include: any illegal activity; any activity involving pornographic material; any activity subject to an adults-only age restriction; software downloads or updates for personally-owned devices.

2.9 The internet connection may not be used for downloading or uploading video or audio data, except for: making video or audio calls as part of normal Council business; recording or streaming of public Council meetings, provided that such recording or streaming has been initiated by the Clerk or a Council-approved delegate; or material required for Council-approved training classes.

Use of the printer

2.10 The printer and the associated supplies of paper and toner are provided exclusively for the business of the Council, such as printing notices of meetings for display on the public noticeboards, or printing documents to facilitate discussion in working groups.

2.11 Employees and councillors may use the printer to print material that is related to Council business, provided there is a reasonable justification for having it on paper.

2.12 The current printer also functions as a scanner. Employees and councillors may use the printer to scan documents that are required for Council business. Scanned documents can be printed or sent to a Council-provided email address.

2.13 No employee or councillor or anyone else may use the printer for anything that is not related to Council business.

2.14 The printer should only be available on the private network. It should never be configured to be visible on the public WiFi network.

2.15 All users are encouraged to print in black-and-white where possible to avoid excessive use of colour toner.

2.16 Management and provision of supplies is the responsibility of the Clerk. Any user who is aware of any shortage of supplies should inform the Clerk. No user should attempt to replace paper or toner cartridges unless they have been properly trained to do so.

2.17 It is customary to print agendas for different committees on different coloured paper. At the Clerk's discretion, a properly-trained employee or councillor may load whatever colour of paper is required, provided that when they have finished, they reload the printer so that the default printing stock for the next user is white A4 paper.

2.18 The current printer requires periodic cleaning and calibration. This is also the responsibility of the Clerk. No user should attempt to do any maintenance, such as cleaning or calibration, unless (a) they are suitably qualified, (b) they have discussed what needs to be done with the Clerk, and (c) the Clerk has given them permission to do the work at a particular time.

Use of the overhead projector

2.19 The overhead projector is provided only to support Council business and should not be used for any other purpose.

2.20 Any councillor or member of staff may connect the usual laptop computer that they use for Council business to the projector, provided only that they have a suitable socket or adapter for the HDMI cable provided. No other form of connection to the projector should be attempted. Users must also position their laptop and the long cable to avoid any trip hazards or other health and safety issues.

2.21 It is recommended that users of the projector format any presentations to 4:3 shape rather than 16:9, so that the projected slides fit better.

3 Use of Council-provided portable equipment

3.1 The council provides laptops and mobile phones to employees for Council business only. The devices are not for personal use, even when they are used at home.

3.2 Each device carries a serial number which will be recorded against the user's name in the device register kept by the Clerk. All devices provided by the Council remain the property of the Council, and each one must be returned in good order when the user ceases working for the council.

3.3 Laptops and mobile phones and any related accessories provided by the Council should be treated with good care at all times. Equipment should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

3.4 Operational problems with any device, including software faults, physical damage, or loss must be reported promptly to the Clerk. Users of devices must not attempt to dismantle or repair a device without first seeking advice from the Clerk.

3.5 Employees must not use any other electronic devices, or accessories, for Council business, without getting prior written authorization from the Clerk.

3.6 Employees must not install any software on laptops or phones provided by the Council without getting prior written authorization from the Clerk. This includes free-to-install apps for mobile phones.

3.7 Laptops and mobile phones must have a PIN or a password enabled at all times, and must be set to lock automatically if not used for more than five minutes. To prevent unauthorized access, users must lock their computers and take their phones with them if they leave their work place temporarily.

3.8 Users must not disable any of these security features and they must not share their device PIN or password with anyone, except to provide for recovery as follows: the PIN or password for each device should be written on an index card, which should be sealed in an envelope marked with the user's name and the device identification details. The envelope should be handed to the Clerk who will store it in the safe on the Council premises.

3.9 Users may enable their own biometric security so that a device can be unlocked more conveniently, but they must only do this for themselves, and they must not disable the PIN or password mechanism.

3.10 Laptops and mobile phones must be stored safely and securely when travelling or working away from the Council office. Equipment must not be left unattended in public areas, and should never be left in parked vehicles, even if locked in the boot.

3.11 External storage devices (SD cards, memory cards, USB sticks, CDs, DVDs, or similar devices) must not be used with any computers provided by the Council without prior approval of the Clerk and the Chair of the Council. The approval should only be granted in exceptional circumstances and only for a specific single purpose within a defined time (such as receiving pictures from a photographer after a Council event).

3.12 Portable devices including laptops and mobile phones must never be used to hold the only copy of any Council documents or records. All devices must be configured to access the Council's cloud-based storage facilities and to make sure that any local copies of documents are automatically synchronized with the cloud-based versions whenever the device is connected. This applies to all files, not just shared files. The essential rule is that the local storage on any portable device can be erased without loss of any Council information.

3.13 All laptops and mobile phones must have disk encryption enabled to prevent access to any data if they are lost or stolen. Where available portable devices should also be programmed to erase all content after several unsuccessful password attempts. Any security set on these devices must not be disabled or removed.

3.14 Users of these devices must set up a new device account using the email address and phone number provided to them by the Council, and using the Clerk's official email address as the recovery contact. The security settings for this account must allow remote finding of each device and allow any device to be locked or erased remotely if it is lost or stolen.

3.15 Users of these devices are responsible for keeping the software on them up to date. Security patches and minor operating system changes should be automatically installed. Major version changes should be done after agreement with the Clerk.

3.16 To protect confidential information, Councillors and staff should not take photographs or videos in the Council office, without the prior permission of the Clerk. This includes mobile telephones with camera function, camcorder, tape, or other recording device for sound or pictures, moving or still.

3.17 Non-public Council meetings or conversations be never be recorded without the express permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

3.18 The Council does not permit webcams (which are built-in to modern laptops and phones) to be used in the workplace, other than for conference calls for council purposes.

4 Use of your own computing devices

4.1 The Council recognises that councillors, and some staff, may wish to use their own computing devices access for council business, including, but not limited to, accessing the Council-provided email service and shared storage. Any such use of personal devices will be at the discretion of the Clerk, but consent for standard systems in commercial configurations will normally be permitted.

4.2 The Clerk will maintain a record of who has been allowed to use a personally owned-device for council business. This record may be needed when answering Freedom of Information requests.

4.3 Users remain financially responsible for their own equipment; the Council will not normally pay for any costs associated with the use of a personal device for Council business.

4.4 Users must ensure that any device used for council business is clean and kept in good order, and that it presents a professional image when used in public.

4.5 Users should keep the operating software up to date on all devices used for Council business, to reduce the chance of introducing malware or creating problems for other users.

4.6 Operational problems with personal devices remain the responsibility of the user, but any problem that might have exposed Council related documents or data to unauthorised users, and any loss or theft of a device must be reported promptly to the Clerk.

4.7 Personally-owned laptops and mobile phones used for Council business should have a PIN or password enabled at all times (in addition to any biometric locking), and must be set to lock automatically if not used for more than five minutes.

4.8 External storage devices (external disk drives, SD cards, memory cards, USB sticks, CDs, DVDs, or similar devices) must not be used for Council business without prior approval of the Clerk and the Chair of the Council. The approval should only be granted in exceptional circumstances and only for a specific single purpose within a defined time.

4.9 Personally-owned laptops or mobile phones must never be used as the only storage location for official Council records. Users of personal devices may keep working copies of documents or plans that they are working on, but not permanent official records. All such devices must be configured to access cloud-based storage facilities and to make sure that any local copies of documents are automatically synchronized with the cloud-based versions whenever the device is connected.

4.10 Personally-owned laptops and mobile phones must never be used to process sensitive personal information (SPI) for the Council. Unlike generic personal data, such as names or email addresses, SPI is data about a person that could be harmful if exposed, and that usually has special legal protection. SPI includes medical details, bank account details, credit card numbers, NI numbers, biometric data, and information about protected characteristics such as ethnic origin, political views, or sexual orientation. Councillors and staff using personally-owned devices for Council business must never process any form of SPI for the Council on their devices.

4.11 All personally-owned laptops and mobile phones used for Council business should have disk encryption enabled to prevent access to any data if they are lost or stolen. Where possible, these devices should also be programmed to erase all content after several unsuccessful password attempts. Any security set on these devices must not be disabled or removed.

4.12 Users of personally-owned laptops and mobile phones should set up a device account that allows remote finding of each device and allows each device to be locked or erased remotely if it is lost or stolen. In the event of loss of a device, users must cooperate with the Clerk in order to avoid unauthorized access to Council systems.

4.13 Users of personally-owned laptops and mobile phones should be aware that in the event of the Council being involved in legal action, or being otherwise required by law to respond to requests for information, the Council may need access to a personally-owned device to retrieve relevant data.

4.14 Users of personally-owned devices should maintain a clear separation between Council-business and personal business. For example, by using different apps for personal email and Council email. Users must always ensure that they always use the Council's email system to send emails about Council business. If the device supports work and personal profiles, an appropriate work profile should be used for Council business.

4.15 Personally-owned laptops should only be used on trusted WiFi networks that are secured with password, such as the network in the Council office or in their own home. Users should avoid doing any sensitive Council business on public-access WiFi networks such as those provided in cafés or on public transport. If in doubt, users should work via the personal hotspot on their mobile phone.

4.16 It is strongly recommended that councillors and staff do not allow friends or family to use a personally-owned device that is being used for council business.

4.17 If a user plans to dispose of any personally-owned device that has been used for Council business, the user should ensure that the device has been completely reset and that all data has been removed before disposing of the device. At the Clerk's discretion, the user may be asked to demonstrate that no Council documents or other data remain on the device.

4.18 If a member of staff or a Councillor leaves the Council, for whatever reason, they should promptly remove all data relating to Council business from any personally-owned devices and from any personal cloud storage services. This should include emails, and personal copies of working documents, but there is no need to remove copies of published material. The principle is that once someone has left the Council, they should have no more access to Council data than any other member of the public. At the Clerk's discretion, the user may be asked to demonstrate that this has been done.

5 Use software systems for Council business

Microsoft Office or equivalent

5.1 Microsoft 365 Business Basic is provided only for employees who need to work with documents and spread sheets, or to make presentations. Councillors are expected to licence their own copies of Microsoft Office or to use equivalent tools such as Libre Office or other open-source document management tools. Users should strive for simplicity and compatibility in documents, spread-sheets, and presentations, so that their colleagues are not locked-in to one product or another.

5.2 Documents for review within the Council may be circulated in PDF format, or the modern native Microsoft formats: (`.docx`, `.xlsx`, or `.pptx`), or in any of the OpenDocument standard formats. The older Microsoft forms (`.doc`, `.xls`, or `.ppt`) should be be avoided.

5.3 Documents published to the website or sent to external recipients via email, must always be published in accessible PDF format, or converted to plain HTML as appropriate. Users should never publish or email documents in Microsoft Office formats.

Shared Storage

5.4 All Council documents and files must be kept on automatically backed-up, highly available cloud-based storage. No individual laptops or phones should ever hold the main copy of any Council data. All devices, whether provided by the Council or personally-owned, should be configured so that any files and folders used for Council business are automatically synchronized to cloud-based storage.

5.5 The Microsoft licences also include a large amount of cloud-based storage per user. It is the responsibility of the Clerk, working with the Assistant Clerk, the Facilities Manager, and any other suitably qualified Councillor or employee to organize this storage, and to make sure that each employee can access the appropriate shared folders.

5.6 The Clerk will maintain a plan to ensure that critical Council records can be restored within a reasonable time following a major system or provider failure.

Email

5.7 All councillors, staff, and other authorised users who need to use email as part of their work with the Council will be given their own Council email address and account. The Council may, at any time, withdraw email access, should it decide that this is no longer necessary for the role or that the facility is being abused.

5.8 Email messages sent on a Council email account are for council business only. Personal use is not permitted under any circumstances. This also works the other way: councillors and staff must never conduct any Council business using a personal email account.

5.9 Employees or councillors with a laptop or mobile phone provided by the Council must not use that device for personal email.

5.10 It is strongly recommended that Councillors and other authorised users who are using their own computers or mobile phones for council business use different apps for Council email and personal email. So for example, an Apple Mac user might use Apple Mail for personal email but use Outlook for Council email.

5.11 All users of the Council email system should also be familiar with using the web-based interface to email, and should regularly log in to this interface to check for quarantined email and to ensure nothing has been missed by the email client on their phone or laptops.

5.12 Council email facilities are intended to promote effective and speedy communication on work-related matters, but all users should be aware of the risks, and all users should follow email etiquette.

5.13 Users of email should be aware of the risks of fake emails. It is a common practice for criminals to send fake emails, usually as an attempt to steal money. Users of the Council email service are at higher risk because their names and email addresses are published on the Council website, along with some biographical details. Criminals can use these details to construct very convincing fake emails. • If you receive an unexpected email purporting to be from a colleague and asking you to do something urgently, do not act on the email before discussing it with a colleague or the Clerk. • Do not open unexpected attachments in emails without speaking to the sender first and getting them to explain what the attachment contains. • Never click on a web link in any email, even from trusted sources like NALC; instead you should hover your mouse over the link to display the URL and then, if it looks correct, copy the URL into your browser.

5.14 Email is much more effective if everyone follows some simple email etiquette.

- Consider talking face to face, or on the phone, instead of writing an email.
- Never send an angry email, instead get up and do something else for an hour, then come back and reword the email politely (or delete it)
- Never say anything about a colleague or a member of the public that you would not say to them directly. Anything you write in an email is essentially public property
- The “reply all” feature should only be used appropriately
- Do not use the BCC field for regular Council business; you must act openly
- But you MUST use the BCC field if you are sending an announcement email to a list of email addresses; the Council has a duty of confidentiality not to share people’s email addresses without their consent
- Try to avoid long quotation chains when replying to an email thread; best practice is to highlight the sentence you want to address before you press the reply button; most email programmes will then put just the highlighted text at the top of your reply, and you can make your point underneath
- Include a short professional signature at the end of your email, with your phone number if appropriate

Payroll and accounting

5.15 Payroll and accounts are essential to the Council's proper function. Payroll and accounts must be done using secure cloud-based professional software that stores all the data securely and backs it up automatically.

5.16 Vital payroll and accounts data should be periodically exported to an encrypted archive copy and stored on an independent cloud-based storage system. Payroll and accounts data should never be stored permanently on any Council-provided laptop or desktop computer, and should never be stored at all on any personally-owned device, unless explicitly authorized by the Clerk for a specific business purpose.

5.17 The Clerk is responsible for maintaining a recovery plan for the payroll and accounting systems. In the event of a catastrophic loss of the cloud-based payroll and accounting systems, such as the failure of the provider or an extended period of unavailability, it is important that the payroll and accounting system should be recovered within 7 working days. The Clerk's plan should explain how this will be done; the plan should also be suitable for migrating the payroll and accounting systems to a different provider.

5.18 User access to the payroll and accounts systems should be protected by two or more different authentication factors – such as a password backed up by an authenticator code.

Website

5.19 The Council's website is the public face of the Council so it must be kept up to date and must be accessible, inclusive, and professional.

5.20 The website consists of three main parts: information about the village and the Council, with links to the District and the County councils; a public repository of meeting minutes and related documents; a contact form that allows members of the public to subscribe to email updates.

5.21 The website should only be updated by the Clerk, or a Council-approved delegate. Major changes to the website content, and especially additions or removals of links to external sites, should be reviewed with the chair of the Communications Working Group.

5.22 Using an appropriate provider, the Clerk should register an appropriate website address, and maintain this registration paying an annual fee as required, and as approved by the Council.

5.23 The website must be presented on a secure port using the standard `https` protocol. The Clerk is responsible for ensuring that the necessary security certificates are correct and kept up to date, paying an annual fee as required and as approved by the Council.

5.24 The Clerk is responsible for maintaining a recovery plan for the Council website. In the event of a catastrophic loss of the website, such as deletion of the source files, or failure of the hosting provider, the Clerk must ensure that a temporary status page is available within two business days, and that a working website is available within 10 business days. This plan will include recovering or recreating the information pages, and re-building the document repository from the Council's shared storage.

6 Use of AI tools for council business

6.1 AI tools are offered freely by search engines to help you find information on the web, by many writing tools to help you draft a report or alter the style, and by email clients to summarize your emails. Councillors and employees must exercise care and judgement before using AI tools, they should inform themselves about what AI is, they should understand how AI tools might help their work, and what limitations the tools have.

6.2 AI tools currently lack reasoning and contextual awareness and their limitations vary depending on the tools you use and the context in which they operate. AI tools are also not guaranteed to be accurate. If you choose to use AI tools you must always find a way to test the accuracy and correctness of their outputs.

6.3 Your use of AI tools must be lawful and responsible. AI models are trained on data which may include biased or harmful materials. As a result, AI systems may display biases and produce harmful outputs, such as unfair, prejudicial or derogatory representations of groups or individuals. You must consider whether the output or decision provided by the tool is objective and fair.

6.4 HM government encourages local councils in the UK to follow the Algorithmic Transparency Recording Standard (ATRS). This means you must publish full details about any algorithmic tools you use in Council business. Even if you are only using a generative text tool to embellish a policy document, you must always add a paragraph with a reference to the tool, and explain how the tool was used and why. For example, a response that has been generated via a chatbot interface should include something like ‘this response has been written by an automated AI chatbot’.

6.5 It is tempting to get AI tools to “improve” an existing text; but you must not submit all or part of any document into an AI tool unless you have the permission of the author or copyright owner.

6.6 The Council will not reimburse staff or Councillors for any expenses incurred for the use of any AI tools, without explicit approval from the Council.

6.7 Staff and Councillors are encouraged to take training classes to gain the skills they need to understand the risks and opportunities of AI, including its potential impact on organisational culture, governance, ethics, and strategy.

6.8 For further information, Councillors and staff are encouraged to review the Artificial Intelligence Playbook for the UK Government available on gov.uk.

7 Data management

7.1 *This section does not deal with the Council's policies in respect of the Data Protection Act 2018 and the Freedom of Information Act 2000; these are set out in the Data Protection Policy document and the Requests for Information policy*.

Dealing with sensitive personal information (SPI)

7.2 SPI is data about a person that could be harmful if exposed, and that usually has special legal protection. SPI includes medical details, bank account details, credit card numbers, NI numbers, biometric data, and information about protected characteristics such as ethnic origin, political views, or sexual orientation.

7.3 Users of personally-owned devices for council business are expressly forbidden from processing SPI for the Council in any form on their devices.

7.4 Users of council-provided phones should avoid processing SPI on these devices.

7.5 Users of council-provided computers should take extra care to avoid exposing SPI. SPI associated with staff payroll should be kept in the cloud-based system, and not routinely copied to local storage. If SPI is required on local storage for a *bona fide* Council-business purpose, it must always be stored in a password-protected file. The passwords must be managed according to the policy guidelines below.

7.6 SPI should never be shared on email or messaging apps. SPI must never be copied to removable storage media.

Back up policy

7.7 Users of personally-owned or Council-provided computers and phones should not routinely take back up copies of their Council-related files or documents. Instead these files or documents should be stored on a cloud-based storage service that is backed up automatically. Computers and phones should be configured so that any local copies of files or documents are automatically synchronized with the cloud-based version whenever the device is connected. Users should not store Council-related files on local storage that is not synchronized to a cloud-based storage service. The guiding principle is that the loss on any one physical device should not cause any data loss to the Council.

7.8 Council staff should use the storage provided as part of their Microsoft 365 licence.

7.9 Councillors may use any commercial cloud storage service. The Council will not reimburse any expenses associated with this type of storage. Councillors are recommended to set up an account with a storage service provider using their Council email address, and to use that storage service exclusively for Council business. This will make it easier to provide access to the Clerk if required, and to demonstrate that the storage has been erased if/when the Councillor leaves the Council.

Use of portable media

7.10 External storage devices (SD cards, memory cards, USB sticks, CDs, DVDs, or similar removable media devices) must never be used for any Council business, neither for data transfer, nor for back up, nor for any other purpose. These devices are too easily damaged or lost or stolen.

Data integrity and recovery

7.11 Any suspected IT or data security incident, including loss or theft of a device, suspected phishing, malware infection, or possible unauthorised access to Council data, must be reported immediately to the Clerk. Such reports will be handled in accordance with the Council's Data Breach Response Plan.

7.12 Creation, retention and deletion of electronic Council records must comply with the Council's Retention and Disposal of Documents Policy and Retention Schedule. Deletion of Council records must be carried out within Council-controlled systems so that disposal actions can be evidenced and audited, and that an audit trail of deletions is maintained.

8 Passwords and authentication

8.1 Passwords are a very poor way to protect any IT system. If they are easy to remember, they are very easy for an attacker to guess. If you make them longer and more complicated, then they are very easy to get wrong and very difficult to use. And yet the Council needs to protect access to systems and data, and no-one working for the Council is allowed to forget a password in case it is needed to answer a Freedom of Information Request. Therefore, all users must set up and use an encrypted password manager for council business. Users may use the built-in Apple password manager, or Google Password Manager, but it is recommended that Council-related passwords are kept in a separate password database. At the discretion of the Clerk, the Council may reimburse individuals for the cost of a password manager if there is no suitable free product available.

8.2 Passwords are personal and must not be shared under any circumstances. Only the assigned user of an account may access or use the associated password. In exceptional cases (incident response or off-boarding), access to system credentials may be granted to the Clerk (or Council-appointed delegate) with appropriate approvals and logging.

8.3 Users may write down important passwords on paper, seal them in a labelled envelope and ask the Clerk to store them in the Council's safe, in case of emergency need.

8.4 Users must never store passwords in any other form, except in a Council-approved encrypted password manager.

8.5 All user accounts should be protected by strong, secure passwords, generated by and stored in the user's encrypted password manager.

8.6 Two-factor authentication must be enabled where it is available. It is recommended to use an authenticator app, but also acceptable to use codes sent to a mobile phone.

8.7 The Clerk must keep an encrypted password manager database for Council-owned hardware devices, such as routers or printers. Default passwords on such devices must be changed before they are used for Council business.

9 Monitoring

9.1 The Council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation.

9.2 The Council reserves the right to monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

9.3 Any information obtained through monitoring may be shared internally, including with relevant councillors and staff if access to the data is necessary for performance of their roles. The information may also be shared externally for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

9.4 Any information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

9.5 The Council reserves the right to inspect files stored on any computer systems used for Council business at any time in order to assure compliance with this policy; this applies to systems provided by the Council and to personally-owned devices.

10 Use of material from the Web

10.1 Much of what appears on the Web is protected by copyright. Councillors and staff should not assume that because a document or file is on the Web it can be freely copied. Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The infringement of the copyright of another person or organisation could lead to legal action being taken against the Council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

10.2 One of the main benefits of the Web is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Users should bear in mind that, as the Web is uncontrolled, much of the information may be less accurate than it appears.

11 Use of social media

11.1 Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, Instagram, TikTok, etc.); text messaging and mobile device communications; and more traditional forms of media such as TV and newspapers.

11.2 The policy for employee's use of social media is set out in the Employee Handbook. Councillors should familiarise themselves with the guidelines in that document, and should aim to set a good example by following the same rules.

11.3 Councillors and staff should also read the Council's Communication Policy and follow the Social Media guidelines set out in that document.

11.4 Councillors may engage with social media to inform and explain any Council business, but they should always bear in mind that the Council has a collective responsibility for all decisions it makes, so they should either be supportive or remain silent. In particular, councillors must not contradict official Council communications. If in doubt, councillors should discuss a topic with the Clerk or with the Chair of the Communications Working Group before they post. Councillors engaging with social media on Council business must clearly identify themselves as councillors.

12 Health and safety

12.1 The council has a legal duty to protect the health of all employees who work with display screen equipment, such as the laptops issued to staff.

12.2 If your work with the Council requires you to work with your laptop daily, and for periods of more than one hour at a time, then the Health and Safety (Display Screen Equipment) regulations apply to your work, and the Clerk will undertake a DSE workstation assessment with you at least every 12 months. The Council will also: provide an annual eye test if you want one; provide Health and Safety training for you; and encourage you to take regular breaks from DSE work.

12.3 If the results of a workstation assessment indicate that you need an external display, or other accessories to improve your DSE work place, this will be provided subject to the approval of the Council.

13 Training

13.1 Councillors and staff must undertake annual IT and cyber-security awareness training as arranged by the Clerk or Council-approved delegate.

14 Sanctions

14.1 The sanctions for anyone who breaches any aspect of this policy depend on what relationship they have to the Council.

14.2 Employees will be subject to disciplinary action, at the discretion of the Chair of the Council and the Staffing Committee, as set out in their contract of employment.

14.3 Councillors may be reported to the Monitoring Officer, at the discretion of the Clerk and the Chair of the Council, following the provisions of the Councillor's Code of Conduct published by South Oxfordshire District Council.

14.4 If a member of the public attending any Council meeting breaches the policy, the Chair of the meeting should immediately suspend the meeting; the Chair and Clerk (or their delegates) should then explain the problem to the person involved and obtain their consent to abide by the provisions of this policy, before the meeting is restarted.

End of document