Introduction

The purpose of this policy is to set out how our staff and volunteers should use the technology that is provided to them at work in order to carry out what is required in their role. It is also to:

- Outline what is required of staff and volunteers in terms of their use of social media and personal IT equipment.
- Raise awareness of the risks associated with using IT and therefore protect the organisation from loss of data and data breaches, in line with our requirements under the General Data Protection Regulation (GDPR).

This policy applies to all Cellar Trust staff and volunteers and covers the use of computers, mobile devices such as laptops and tablets, internet use, remote access connections, email servers, file storage, webmail, software, mobile phones and land line telephones.

Related Policies

- Code of Conduct
- Confidentiality Policy
- Data Protection Policy
- Disciplinary Policy
- Equal Opportunities and Diversity Policy
- Grievance Policy
- Privacy Policy
- Social Media Policy
- Whistleblowing Policy

Roles and Responsibilities

Employee	• Adhere to professional and personal standards and good working practices. • Report any breaches of this policy to their line manager.
Line Manager	• Ensure staff are adhering to this policy and follow any disciplinary processes where necessary
Chief Executive Officer (CEO)	• Advise and support managers in the application of this policy and procedure.
Trustees	• Ultimate responsibility for ensuring the correct policies and procedures are in place for recruiting and managing staff and volunteers.

Use of Work IT Equipment

- All computer systems are password protected. Password protection is activated whenever a workstation is left unattended. Passwords are changed regularly (at least every three months).
- All Cellar Trust laptops, tablets and memory sticks are encrypted.
- Memory sticks must not be used to save personal information relating to individuals.

- All data or documents should be saved to the server. No data should be saved to desktop as it is not protected by our backup and security systems.
- Under no circumstances should any computer equipment be tampered with. The removing of any casing or any electronic components is prohibited. Any changes to the system configuration must be carried out by authorised personnel only. Any faults detected must be reported immediately to the Operations Manager or line manager.
- Any movement of equipment should be arranged with the Operations Manager or line manager to ensure that the organisation's inventory is maintained.
- No external equipment should be brought into the organisation and plugged into The Cellar Trust network without discussion with your line manager and / or the Operations Manager.
- On no account should any software, including games, screensavers, etc. be installed onto a computer without the consent of the individual's line manager (advice can be sought from The Cellar Trust IT support if necessary).
- All licensing rights are held by the Cellar Trust. Staff should be aware that the copying of software, music, DVD's etc. is prohibited unless an appropriate licence is held for that purpose.
- Staff must not use work equipment to carry out excessive printing for personal purposes.
- Work mobile phones - Staff who are required to use a mobile phone for work purposes will be provided with access to a work mobile phone.
- Staff who use work mobile phones must ensure that they use fingerprint recognition or have an access pin code set on the phone.
- Staff must not use work mobile phones for personal purposes except in an emergency. Any cost arising from any unauthorised personal use may be repayable by the employee and may result in disciplinary action in accordance with our procedures. The Cellar Trust reserves the right to deduct the appropriate sums from your pay in the event that repayments are not made.
- If staff are required to contact clients using their work mobile phone they must keep messages to a minimum and the main purpose will be to arrange or cancel appointments.
- The Cellar Trust reserves the right to monitor all communications made on work mobile phones in order to ensure compliance with our policies and procedures.
- Landline phones - Staff are not allowed to make personal phone calls on the Cellar Trust landline phones unless in exceptional circumstances which should be pre-authorised by their line manager. Anyone found to be making excessive personal phone calls may face disciplinary action.
- Staff are also reminded that they must be mindful of the organisation's Confidentiality Policy when making and receiving phones calls and if necessary make arrangements to have private space to discuss sensitive details.

Use of Personal IT Equipment

- Staff should only use personal devices to complete work tasks (laptops, PCs or tablets) where necessary. In these cases staff must only use the remote access software to connect to the server which provides the same levels of security as working on site.
- Staff must not store any Cellar Trust data or documents on personal devices.

- Personal mobile phones – Ideally staff must not use their personal mobile for work purposes. If it is agreed by their line manager that they can use their personal mobile phone they may be able to claim expenses in accordance with the Cellar Trust Expenses Policy.
- It is expected that staff will only use their own mobile phones for personal reasons during breaks where possible; however it is understood that there may be occasions where staff need to respond to calls or messages during work hours and this will be allowed if done appropriately and with minimal impact on their productivity. Excessive and/or inappropriate use of personal phones whilst at work may result in disciplinary action

Authorisation

- All individually allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they have been allocated. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person, other than to designated members of IT support staff for the purposes of system support.
- Any attempts to access, or exploit any username, e-mail address, which is not authorised to the user, are prohibited. No one may use, or attempt to use IT resources allocated to another person. All users must correctly identify themselves at all times. A user must not masquerade as another or withhold their identity.
- A user must take all reasonable precautions to protect their resources. In particular passwords used must adhere to current password policy and practice.
- No passwords should be auto saved for any online or IT system (e.g. Lamplight, HR Online, staff training sites, Office 365 webmail).
- The Cellar Trust reserves the right to access the individual email accounts of members of staff if they are on an extended period of sickness absence and to divert their email so as to ensure that operations can be maintained.

Internet

- Employees may use internet facilities for occasional personal matters, but must not access social media for personal purposes unless during the lunch or designated break periods.
- In particular, employees must not use The Cellar Trust facilities to create, display, produce, store, circulate or transmit obscene, derogatory, offensive, discriminatory or pornographic material in any form or medium.
- It is also inappropriate to use IT equipment in a manner that interferes with your productivity or the productivity of others.
- If any staff member is found to be accessing inappropriate content or to be using the internet excessively they will be in breach of this policy and may face disciplinary proceedings.
- Staff must not use the pubic Wi-Fi to access anything work related as this is not a secure connection; only the staff secured Wi-Fi network should be used if required.

Use of Social Media

This is covered in The Cellar Trust Social Media Policy.

Email

All emails are held through Office 365, a cloud-based encrypted email system meaning staff have access from any computer or device with internet access.

Sending internal emails
Staff are required to refrain from identifying clients using their full names in any internal emails and from emailing any personal data to colleagues. If it is necessary to email a colleague about a client then staff must use either initials or RIO numbers and refer colleagues to Lamplight (the Cellar Trust cloud based client management system) where we store client files and case notes.

Sending external emails
Where possible staff are required to refrain from emailing client data externally; however due to the services we provide and in line with specific data sharing agreements in place, it is sometimes necessary to share data with other agencies and professionals (with the clients consent or in the case of risk of harm to self or others). Before sending any personal data externally you must carry out checks to ensure you are satisfied the person is who they say they are and have a genuine reason for requesting that data. You must also ensure that sharing that data meets any GDPR, data protection and consent requirements. In these instances staff must only send client data in WinZip files which are encrypted.

Using outlook calendars

All staff are expected to use shared Outlook calendars for diary management. Staff must not input personal data into their calendar unless it is necessary to do so, for e.g. client initials should be used not full names. The exception to this is if it is necessary for lone working practices. Staff are reminded that they must adhere to The Cellar Trust data protection and confidentiality policies at all times.

Using Email Safely

Hackers and criminals sometimes use unsolicited emails that contain attachments or links to try to trick people into providing access to information. This type of threat is known as phishing. If you receive a request from a supposed colleague asking for login details or sensitive, financial or client information, you should always double-check the request with the colleague over the phone.

Equally, if you receive an unsolicited email that contains attachments or links that you have not asked for, do not open them. Remain vigilant and report the suspicious email to your line manager, a member of the Leadership Team or the Data Protection Officer.

Phising

Criminals use phishing emails and websites to scam people. They are hoping that you will click on fake links to sites or open attachments so that they can steal data or install malicious software. Phishing email attachments or websites might ask you to enter personal information or a password, or they could start downloading and installing malware.

Do not install any new software unless you are advised to do so by your line manager or IT support. If you have any concerns please report these immediately to your line manager or IT support.

Macros, Malware and Websites

Macros
Macros are a series of actions that a programme such as Microsoft Excel may perform to work out some formulas. Your computer will disable macros by default because they can be programmed to install malware. Always be vigilant when enabling macros and ensure you trust the source of the document?

Malware
Malware should be prevented by the organisation's anti-virus protection however there are still threats from this type of malicious software. Malware can make computers run slowly or perform in unusual ways. If you suspect that your computer is not performing as it normally does, contact your line manager or IT support.

Websites
Be vigilant when you visit a website that is declared 'untrusted'. If a web browser states that you are about to enter an untrusted site, be very careful. It could be a fake phishing website that has been made to look genuine. A browser may display a red padlock or a warning message stating your connection is not private.

Security and Back Up

The Cellar Trust uses the following systems and processes to ensure the security and protection of all our electronic data:

- Microsoft Office 365 exchange online - a Microsoft cloud based email solution which includes industry standard virus and malware protection.
- Kerio Control – a unified threat management (UTM) firewall to prevent hackers and security attacks or breaches.
- Eset – virus protection on all PCs and laptops. Staff using personal devices must show they have adequate virus and malware protection.
- Remote access – Virtual Private Network (VPN) access is controlled by Kerio control. All remote workers connect into the building via a secure and encrypted VPN connection. Passwords work the same way as detailed above.
- Back up of electronic data – all data is saved onto The Cellar Trust server and synced to our internal RAID ARRAY system to protect against hardware failure (Sage account data is backed up daily by the Finance Manager onto a folder on server that only this person has access to).
- Every night there is an automatic back up taken from the RAID ARRAY to our external back up servers to ensure data is not lost in the event of a fire or theft.
- We do not hold any data outside the European Economic Area. Our data is encrypted and stored in a data centre based in London; our emails are provided by Microsoft and their servers are based in Holland.
- IT hardware that contains data is disposed of in accordance with strict data protection processes. This is done by a third party who provide a certificate to show it has been wiped or disposed of correctly. Copies of these certificates are kept.

Passwords

It is important to use strong passwords on all of your devices to prevent unauthorised access. You should also use different passwords for each account or system you are using.

The National Cyber Security Centre (NCSC) https://www.ncsc.gov.uk/ has a range of guidance on good password management.

Misuse

Misuse of IT facilities and/or breach of this policy may potentially result in disciplinary proceedings and dismissal. Examples of misuse include:

- Not adhering to The Cellar Trust IT Policy.
- Viewing or downloading inappropriate internet content.
- Excessive use of the internet for personal purposes.
- Inappropriate use of social media which may bring The Cellar Trust into disrepute or break organisational confidentiality rules.
- Attempting to discover a user’s password.
- Using the computer systems to act abusively.
- Attempting to circumvent the network’s security.
- Knowingly running and installing programmes intended to damage the computer systems.
- Deliberately wasting computer resources.
- Leaving laptops or tablets unattended in a public place or otherwise not following the required security protocols.
- Sending client data or personal information in emails without using the proper security controls.