	People and Culture Committee
	13th July 2023
	September 2023
	September 2024

- The UK General Data Protection Regulation
- Computer Misuse Act 1990

10.

10.1 You must not use public Wi-Fi to connect to the internet on a WAT device. For example, if you are working in a public space then you will either need to work offline or use 3G / 4G.

10.2 All use of the Internet is governed by a legal agreement with our Internet Service Provider (ISP) in addition to the guidelines here. If you use a personal computer at home for work purposes, you must ensure that any WAT-related sensitive or personal information is secured to prohibit access by any non-member of staff and encrypted to protect against theft.

11.1 WAT has a set of procedures for the automatic backing up, accessing, and restoring of all data held on school systems, including off-site backups, use of “Cloud Based Storage Systems'' (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected. WAT will ensure that appropriate industry standard controls and encryption are in place by remote /cloud-based data services providers to protect all data.

11.2 Private cloud storage or file sharing accounts must not be used to store or share WAT documents.

11.3 When using shared drives such as google, the appropriate levels of access must be managed and controlled and restricted to people who require access on a “need to know” basis only.

12.1 Users of WAT equipment must not use, down stall any software, app me, or service without permission from the IT support

12.2 Users must not connect (whether physically or by ther method i-Fi or Bluetooth) any device or hardware to WAT IT systems without p .

13.1 All users must use WAT’s systems responsibly. The followin d use of the trust’s IT facilities and any unacceptable or inappropri will be considered under the Code of Conduct and may be subjected to dis acti

- Using the trust’s IT facilities to breach intelle perty rights ght.
- Using the trust’s IT facilities to bully or ha one else, or t unlawful discrimination
- Any illegal conduct, or statements wh emed to be advocating tivity.
- Using, transmitting, or seeking inap or offensive materials.
- Accessing, creating, storing, linki nding material that is pornogra nsive, obscene or otherwise inappropri
- Sharing confidential informati e trust, or any members of the trust’s .
- Connecting any device to tr

ış to

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trustö l

-

- If travelling by public transport, t

23.1 It is the role of the IT Support Team to ensure that WAT’s computer systems are working optimally at all times and that any faults are rectified as soon as possible. Any problems should be reported to the IT support team.

23.2 If you suspect that your computer has been affected by a virus or other malware, you must report this to a member of the IT Support Team immediately.

24.1 Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff and be used

2.6 The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged, and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

  - The contents of the payment card magnetic stripe (track data) on any media whatsoever.
  - The CVV/CVC (the 3- or 4- digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
  - The PIN or the encrypted PIN Block under any circumstance.

- All data must be securely disposed of when no longer required, regardless of the media or application type on which it is stored.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A termly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “Confidential Waste” - access to these containers is restricted. The destruction of all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The destruction of electronic data will require that it be unrecoverable when deleted.

- All machines must be configured to run the latest anti-virus software as approved by WAT. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use will be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- End users must not be able to remove or adversely change the settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail

system as well as from the trash bin. No one should forward any email