Windsor Academy Trust

Policy: Information Security and Acceptable Use Policy (for Staff)	
Responsible Committee:	People and Culture Committee
Date approved by the Board of Directors:	13th July 2023
Implementation date:	September 2023
Next review date:	September 2024

1. Introduction

1.1 This policy aims to support and reinforce Windsor Academy Trust's (WAT) policies and should be read in conjunction with the following:

- Information and Records Retention Policy
- Data Breach Policy and Procedure
- E-Safety Policy
- Code of Conduct
- Privacy notices for staff, students/pupils and parents/carers.

1.2 This policy applies to all employees, members, directors, Local Advisory Body (LAB) members, agency staff, contractors, work experience students and volunteers when handling information and Personal Data.

1.3 Any questions or concerns about obligations under this policy should be referred to the appointed Data Protection Lead (DPL) for each academy or the Data Protection Officer (DPO).WAT has appointed Judicium Education, a company that specialises in data protection, as the trust Data Protection Officer. Judicium will support the Director of Operations in the development and implementation of data protection policies. Judicium contact details are on the WAT website. Any questions relating to the use of Information Technology (IT) should be raised with the IT manager/support team.

1.4 The key areas relating to information security covered in this policy include organisational security and how users engage with and operate paper base and computer-based systems and technical security relating to ensuring that systems used have inbuilt security and protection.

2. Personal Data

2.1 Data protection is about protecting information about individuals. Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.

2.2 Even something as simple as a person's name, their birthday or hobbies count as their Personal Data. WAT's Data Protection Policy provides further information relating to WAT's obligations outlined in the UK General Data Protection Regulation (UK GDPR). Anyone accessing or processing personal data has to follow strict rules called "data protection principles" to ensure that information is used fairly, lawfully and transparently.

3. Information Security

3.1 Information security is about safeguarding the Personal Data relating to individuals and protecting other information that is confidential or sensitive. Information security is important as it protects WAT's ability to function and the data that WAT collects. Having an appropriate level of IT security enables the safe operation of applications and safeguards the technology being used. IT systems are now used extensively in the delivery of teaching and learning, pastoral and professional services and the administration of the trust.

3.2 All systems used present challenges as risks can materialise due to lack of effective security and/or due to the working practices of system users. Data breaches often occur due to human and system errors or weaknesses that can lead to unauthorised access to information and data. Whilst IT is a critical resource in keeping data safe, information security is applicable to paper based as well as computerised systems enabling WAT's operations.

3.3 WAT will ensure that appropriate security measures are in place to prevent unauthorised individuals gaining access to Personal Data and confidential or sensitive information as required by the following:

- The UK General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for schools

3.4 Due to the sensitive nature of card processing activities, the Payment Card Industry Security Standard Policy (PCI-DSS) is also included as an appendix (1) to this policy.

4. Organisational Security

4.1 Appropriate physical security must be in place with visitors being received and supervised at all times in premises where Personal Data and any confidential or sensitive information is processed and stored.

4.2 Portable computer equipment (such as laptops, chrome books, iPads, digital cameras, or portable projectors) and any other media used to store data must be securely stored for example in a locked drawer, cupboard and/or room when left unattended.

4.3 Papers which contain Personal Data and confidential information must also be locked away in a secure location and never left unattended. Manual filing systems must be held in secure locations and only accessed on a "need-to-know" basis.

4.4 Paper records containing all Personal Data or confidential or sensitive information must be disposed of securely in accordance with WAT's Information and Records Retention Policy. Documents must be placed in confidential waste bins stored in a secure location or by ensuring that all documents have been shredded and disposed of securely. Documents containing Personal Data or any other confidential information should never be placed in the general waste.

4.5 When printing documents, secure print should be set until ready to release the documents and only accessed by the authorised user. If printing or photocopying on a shared printer, check that nothing has been left behind, including original copies of documents.

4.6 Confidential material must be sent by secure post or encrypted if sent by email. Double-check letters to ensure that the right letter is in the right envelope before posting them. Put a return address on the back of the envelope. If the letter goes to the wrong address the person who receives it by mistake can return it without opening it.

4.7 When sending information externally, extra care should be taken to ensure that it is being sent to the correct recipient.

5. Technical Security

5.1 Computer systems must have user-type profile password controls and, where necessary, audit and access trails to establish that each user is fully authorised. All users will be informed about overall security procedures and the importance of following these.

6. Software Updates, Firewalls, and Anti-virus Software

6.1 All WAT IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. Any personal devices using any of the Trust's network(s) must all be configured in this way.

6.2 Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards that have been put in place to maintain and protect Personal Data, information and IT facilities.

7. Setup and Access to Facilities and Materials

7.1 Systems will be set up so that protected files are hidden from unauthorised users. Users will be assigned a clearance that will determine which files are accessible to them. Restricted access to protected data will be controlled according to the role of the user.

7.2 All users of WAT IT facilities will have clearly defined access rights to Trust systems, files, and devices. These access rights are either managed by the IT team directly or by the "owner" of any file sharing drives, folders, and documents (e.g., google file sharing.)

7.3 Users should not attempt to access systems, files, or devices to which they have not been granted permissions. If access is provided in error, they should alert the IT support team immediately who will also liaise with the DPL or the DPO to consider whether there has been a data breach.

7.4 Users should log out of systems and lock their equipment, when they are not in use to avoid the risk of any unauthorised access. Equipment and systems should be logged out of and closed completely at the end of each working day.

7.6 Equipment should be set up so that screens are not visible to other parties, particularly when personal and confidential data and information is being processed.

7.7 If you are doing an online presentation to a group of people, close your emails and messaging services before sharing your screen with others.

7.8 When using video conferencing technology you should make use of privacy and security features. These can include restricting access to meetings using passwords, controlling when people can join the meeting or controlling who is allowed to share their screens. Think about who and how you share the meeting ID or password. Don't click on links or attachments you were not expecting or from meeting attendees you do not recognise.

7.9 Users should contact their IT Support Team for any specific guidance on the information security requirements and setup.

8. Encryption

8.1 To provide an increased level of system security, all devices and systems must have an appropriate level of encryption as installed by the IT manager/support team.

8.2 Staff may only use personal devices to access trust data, work remotely, or take Personal Data or confidential or sensitive information away from WAT sites if they have been specifically authorised to do so by the headteacher/ member of the executive team.

8.3 The use of personal devices will only be authorised if the devices have appropriate levels of security and encryption. All WAT data and information must be kept secure at all times.

9. Internet access

9.1 The school wireless internet connection is secure and uses the latest industry standard security. Bring your Own Devices (BYOD) facilities are also segregated and run secure profiles.

10. Public Wi-Fi:

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. Cloud storage

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. Downloading Software or Connecting to other Devices

12.1 Users of WAT equipment must not use, download, or install any software, app, programme, or service without permission from the IT support team.

12.2 Users must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to WAT IT systems without permission.

13. Use of IT facilities

13.1 All users must use WAT’s systems responsibly. The following is considered **unacceptable** use of the trust’s IT facilities and any unacceptable or inappropriate use of systems will be considered under the Code of Conduct and may be subjected to disciplinary action.

- Using the trust’s IT facilities to breach intellectual property rights or copyright.
- Using the trust’s IT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Using, transmitting, or seeking inappropriate, or offensive materials.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Sharing confidential information about the trust, or any members of the trust’s community.
- Connecting any device to trust IT network(s) without authorisation.
- Setting up any software, applications, or web services on the trust’s network(s) without authorisation or creating or using any programme, tool or item of software designed to interfere with the functioning of the IT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network or drives or to any password-protected information, without approval.

- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trust's IT facilities.
- Causing intentional damage to IT facilities.
- Removing, deleting, or disposing of IT equipment, systems, programmes or information without permission.
- Accessing, modifying, or sharing data (including Personal Data) to which a user is not required to have access.
- Promoting a private business, unless that business is directly related to the trust.
- Using websites or mechanisms to bypass the trust's filtering mechanisms.
- Intentionally damage, disable, or otherwise harm the operation of systems.
- Excessive downloading of material from the Internet.

13.2 This is not an exhaustive list. and there may be other examples that may warrant further investigation and consideration for disciplinary action if appropriate.

13.3 WAT's Child Protection and Safeguarding and E-Safety policies contain additional information relating to safeguarding and online safety with acceptable use agreements, that should also be read in conjunction with this policy.

13.4 In exceptional circumstances only, where the use of Trust IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the executive/ headteacher's discretion only.

14. Passwords

14.1 All users should set strong passwords for their accounts and keep these passwords secure. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

- **Passwords must not be disclosed to anyone**, including IT support staff. If passwords have been disclosed, the password must be changed immediately.
- **Passwords should contain a string of different characters.** Do not choose a password which is so complex that it's difficult to remember without writing it down.
- **Passwords should be difficult to guess**. Do not use information which other people might know, or be able to find out, such as an address or birthday.
- **Passwords should be set for different accounts.** For example, do not use the same passwords for private email addresses or online services for WAT accounts.
- **Passwords (and any other security credential such as a key fob or USB drive) must be kept secure and confidential** and must not be shared with, or given to, anyone else.
- **Passwords should not be written down and should be changed regularly.**

15. Email

15.1 All email sent should contain name, job title and contact details.

15.2 There are a number of considerations when communicating by email as email is not a secure method of communication, and can be easily copied, forwarded and archived. Email has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Email to outside organisations has the same power to create a binding contract as hardcopy documents.

15.3 When using email as a method of communication: the following must be considered:

- **Private email addresses must not be used for WAT-related work**. If communicating with a student/pupil via email, the WAT account must be used.
  Emails to multi recipients must not identify other recipients and must be sent securely. Caution should be exercised when using blind copying (bcc) emails to avoid entering email addresses in the cc field rather than the bcc.
- **Encrypt internal and external emails which contain Critical Personal Data or any other confidential or sensitive information.** For example, when sending details of a safeguarding incident to social services.
- **Do not send or forward chain letters or unsolicited commercial e-mail** (also known as SPAM).
- **Disable autofill in your email settings.** If email addresses come up automatically when starting a new email message. Always double-check recipients before pressing send. Consider entering the email addresses for recipients after drafting the email.

15.4 Email users should, where practical, activate the two-factor authentication on their accounts as an additional security measure.

16. Portable Media Devices

16.1 Portable devices such as USB drives/HDDS should not be used, and users should make use of the trust's provided cloud storage arrangements. If in exceptional circumstances a portable media is utilised only devices that have been authorised and provided by the Trust should be used and the IT Support Team will protect any portable media device issued with encryption. Any devices that have not been encrypted must not be used.

16.2 Personal Data or confidential or sensitive information must not be stored on a portable storage system (such as a USB memory stick, portable hard disk, or personal computer) unless that storage system is encrypted and has been approved for such use.

16.3 If a USB stick is found, please pass to an IT Support Team immediately. Do not plug into a computer.

17. Using personal devices for WAT work

17.1 Personal devices (such as laptop or smartphone) can only be used for WAT work if permission has been granted by the executive/headteacher. Before using any personally owned devices the IT support team must be contacted so that they can configure the device as required.

17.2 Private equipment must not be used to store Personal Data or confidential or sensitive information. This is because anything saved to the computer, tablet or mobile phone will not be protected by WAT's security system and it is often very difficult to delete something which has been saved to a computer. For example, if a document is saved to a laptop because you wanted to work on it over the weekend, then the document would still be on the computer hard drive even if it has been deleted and emptied the recycle bin. Accessing WAT's own network is far more secure and significantly reduces the risk of a security breach.

17.3 The IT support team will ensure that software that has remote wipe functionality can be invoked should the device be lost or stolen. WAT reserves the right to monitor, review and erase all content on the device that has been created for WAT or on WAT's behalf. It may not be possible to distinguish all such information from any private information in all circumstances. Users should regularly back up any private data contained on the device or keep private material separate via a partition that would not be remotely wiped in these circumstances.

17.4 Users must not do anything which could prevent any software installed by WAT on their computer or device from working properly. For example, the software must not be uninstalled, or documents saved to an unprotected area on the device, without contacting the IT Support Team.

17.5 Steps must be taken to ensure that others who use the same personal device (ie. ~~g.~~ friends or family) cannot access anything WAT- related on the device. For example, login details must not be shared, and users must log out and close down after use.

17.6 Devices must be configured in a way that would deny access to WAT related documents and information by unauthorised users. Further advice and information is available by contacting the IT support team.

17.7 If the device ceases to be used for WAT work, all WAT documents (including WAT emails), and any software applications provided by WAT for WAT purposes must be removed from the device.

17.8 All WAT IT equipment (for example laptops, printers, phones, and DVDs) must always be returned to the IT Support Team even if considered broken.

18. Personal Use of WAT Equipment

18.1 Personal use of WAT issued IT equipment is permitted but its use must comply with all other conditions of this policy and all associated WAT policies. Personal use **must not:**

- interfere in any way with your duties or those of any other member of staff;
- have any undue effect on the performance of the computer system; and
- be for any commercial purpose or gain unless explicitly authorised by the trust.

18.2 Personal computer equipment must not be connected to a WAT computer equipment without prior approval from IT staff, with the exception of storage devices such as USB memory sticks (see section 16 on the use of portable media devices).

18.3 You should not save sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).

19. Working Off Site/ Remotely

19.1 Personal Data may need to be taken off site for various reasons, for example working remotely or supervising an academy trip. When working away from WAT sites, only the minimum amount of information should be taken. Critical Personal Data/Special Category Data as outlined in the Data Protection Policy should not be taken off site in paper format save for specific situations where this is absolutely necessary. For example, a teacher organising a field trip might need to take with them information about pupil/student medical conditions (such as allergies and medication). If only eight out of a class of twenty pupils/students are attending the trip, then the teacher should only take the information about the eight pupils/students.

19.2 The trip organiser should decide what information needs to be taken, who will be responsible for looking after it and the arrangements for keeping it secure. Any Personal Data taken off site must be returned.

19.3 Working on documents containing Personal Data whilst travelling is only permitted in exceptional cases where prior permission has been granted. If working on a laptop on a train for example, you should ensure that no one else can see the laptop screen and devices must never be left unattended.

19.4 If hard copy (i.e. paper) records containing any Personal Data or confidential or sensitive information are taken off WAT sites, then documents must be kept safe and secure at all times.

- Documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g., overnight).

- If travelling by public transport, the documents must be kept with you at all times, and they should not be stored in luggage racks.

- If travelling by car, documents must be kept out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when vehicles are stationary e.g., at traffic lights.

- If there is a choice between leaving documents in a vehicle and taking them with you (e.g., to a meeting) then you should usually take them with you and keep them on your person in a locked case. The risks of this situation should be reduced by only having the minimum amount of Personal Data with you.

20. Supervision of Pupil/ Student Use

20.1 Pupils/students must be supervised at all times when using WAT computer equipment. When arranging use of computer facilities for pupils/students, you must ensure supervision is available.

20.2 Academies need to ensure that there is an Acceptable User Agreement In place for pupils/students and implement the requirements as outlined in the WAT E-Safety Policy. Supervising staff are responsible for ensuring that these arrangements are enforced.

20.3 Supervising staff must ensure they have read and understand the separate guidelines on E-safety, which pertains to the child protection issues of computer use by students/pupils.

21. Monitoring

21.1 Use of WAT's computer systems, including email account and storage areas provided may be monitored by the trust to ensure compliance with this policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, records of sites visited on the Internet by both students and staff are kept; however, usernames and passwords used on those sites are NOT monitored or recorded.

21.2 WAT may also use measures to audit use of computer systems for performance and diagnostic purposes.

22. Confidentiality and Copyright

22.1 All users are responsible for complying with copyright law and licences that may apply to software, files, graphics, documents, messages, and other material you wish to use, download, or copy. Even if materials on WAT's computer system or the Internet are not marked with the copyright symbol (©), it should be assumed that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

22.2 You must consult a member of the IT Support Team before placing any order of computer hardware or software, or obtaining and using any software you believe to be free, this is to check that the intended use by WAT is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have).

23. Reporting Problems with the Computer System

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. Portable Appliance Test of Equipment

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 **must not** be used until approved. This test must be performed at regular intervals as required by the trust's normal rules on electrical safety testing.

25. Information Security Breaches

25.1 All security incidents, breaches and weaknesses should be reported to the DPL/DPO as outlined in the Data Breach Policy and Procedure.

26. Breach of this policy

26.1 Any breach of this policy will be taken seriously and may result in disciplinary action.

27. Policy Review

27.1 This policy will be reviewed in line with the review frequency of all Data Protection-related policies.

Appendix 1

Payment Card Industry Data Security Standard (PCI-DSS) Compliance Policy

1. Policy Statement

1.1 All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures set out in this policy. No activity may be conducted, nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

2. Specific Policy Requirements

Network Security

2.1 All card payment terminals are mobile and not connected to the network, card data is also not stored electronically on the network.

- Firewalls are fully implemented to the network.
- Firewall and router configurations must restrict connections between untrusted networks.
- Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- No direct connections from the Internet to the cardholder data environment will be permitted. All traffic has to traverse through a firewall.

Cardholder Data

2.2 All sensitive cardholder data stored and handled by WAT and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the trust for business reasons must be discarded in a secure and irrecoverable manner.

2.3 If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.

2.4 Card holder data (PAN, track data etc.) must never be sent over the internet via email, instant chat, or any other end user technologies.

2.5 If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.).

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.

2.7 It is strictly prohibited to store:

- 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.

Disposal of Stored Data

- 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.

Maintenance of Vulnerability Management Program

- 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, which they suspect may contain viruses.

Access Control Measures

- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices receive training and are restricted to only those necessary for business purposes.
- Any 3rd party maintenance, updates or device replacement is arranged centrally by the finance manager only and the validity of any work is verified prior to work being carried out.
- Terminals are kept locked in either a secure room or safe outside of business hours, during business hours all terminals are in the constant presence of an employee and not left unattended.
- All receipts are kept securely during day-to day operations and then transferred to the finance office for secure storage.