Windsor Academy Trust

Windsor High School and Sixth Form

Policy: Information Security and Acceptable Use Policy (for Staff)	
Responsible Committee:	Windsor Academy Trust, Board of Directors
Date revised by the Board of Directors:	July 2019
Implementation date:	September 2019
Next review date:	September 2021

1. Introduction

1.1 Information security is about what you and Windsor Academy Trust (WAT) should be doing to make sure that **Personal Data** is kept safe. This is the most important area of data protection to get right. Most of the data protection fines have come about because of information security breaches.

1.2 WAT is ultimately responsible for how you handle personal information. In this policy, we refer to the term "WAT" to mean both academies and the central team.

1.3 This policy should be read alongside WAT's Data Protection Policy which gives an overview of your and WAT's obligations around data protection. In addition to the Data Protection Policy, you should also read the following which are relevant to data protection:

- Information and Records Retention Policy.
- Data Breach Policy and Procedure
- WAT's privacy notices for staff, student/pupils and parent/carers; and

1.4 This policy includes information previously outlined in the WAT Acceptable Use and Personal Data Handling Policies. The policy applies to all staff (which includes Directors, Trustees, Local Advisory Bodies (LAB) members, agency staff, contractors, work experience students and volunteers) when handling Personal Data. For more information on what Personal Data is, please see WAT's Data Protection Policy.

1.5 Any questions or concerns about your obligations under this policy should be referred to the appointed Data Protection Lead (DPL) for each academy or the Data Protection Officer (DPO) appointed for the Trust. If you have suggestions on how information security can be improved please let them know.

1.6 Due to the data sensitive nature of card processing activities, the Payment Card Industry Security Services Policy is also included at appendix 2 to this policy.

1.7 Impact levels and protective marking information is also held as an appendix 3 for information.

2. Be aware

2.1 Information security breaches can happen in a number of different ways. Examples of breaches which have been reported in the news include:

- an unencrypted laptop stolen after being left on a train;
- Personal Data taken after website was hacked;
- sending a confidential email to the wrong recipient; and
- leaving confidential documents containing Personal Data unattended.

2.2 These should give you a good idea of the sorts of things which can go wrong, but please have a think about what problems might arise in your team or department and what you can do to manage the risks. One option is to have team specific checklists to help ensure data protection compliance.

2.3 You should immediately report all security incidents, breaches and weaknesses to the DPL/DPO. This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unlocked at weekends).

2.4 You must immediately inform the DPL/DPO if you become aware of anything which might mean that there has been a security breach and provide them with all of the information you have. All of the following are examples of a security breach:

- you accidently send an email to the wrong recipient;

- you cannot find some papers which contain Personal Data; or
- any device (such as a laptop or a smartphone) used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

2.5 In certain situations WAT must report an information security breach to the Information Commissioner's Office (ICO), the data protection regulator and let those whose information has been compromised know within strict timescales. This is another reason why it is vital that you report breaches immediately.

3. Thinking about privacy on a day to day basis

3.1 You should be thinking about data protection and privacy whenever you are handling Personal Data.

3.2 WAT is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. For example, when we introduce new technology, where the processing results in a risk to individual's privacy or where Personal Data is used on a large scale, such as CCTV.

3.3 These assessments should help WAT to identify the measures needed to prevent information security breaches from taking place.

4. Critical School Personal Data

4.1 Data protection is about protecting information about individuals. Even something as simple as a person's name, their birthday or hobbies count as their Personal Data. However, some Personal Data is so sensitive that we need to be extra careful. This is called **Critical School Personal Data** in this policy and in the Data Protection Policy. Critical School Personal Data is:

- information concerning child protection matters;
- information about serious or confidential medical conditions and information about special educational needs;
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
- financial information (for example about parents/carers and staff);
- information about an individual's racial or ethnic origin; and
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- genetic information;
- sex life or sexual orientation;
- information relating to actual or alleged criminal activity; and
- biometric information (e.g. a pupil's fingerprints following a criminal investigation).

4.2 Staff need to be extra careful when handling Critical School Personal Data.

5. Minimising the amount of Personal Data that we hold

5.1 Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe.

6. Acceptable use of IT

6.1 WAT has provided computers and IT devices for use by staff as an important tool for teaching, learning, and administration purposes. Use of computers and IT devices, by both members of staff and students, is governed at all times by this policy.

6.2 All members of staff have a responsibility to use WAT computer systems in a professional, lawful, and ethical manner. Deliberate abuse of these computer systems may result in disciplinary action (including possible termination of employment), and civil and/or criminal liability. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the DPL/DPO. Please also refer to the following WAT polices which provide further information about the use of IT, including social media:

- Child Protection and Safeguarding Policy
- Social Media Policy
- E-Safety Policy
- Staff code of Conduct

6.3 You **must not allow a pupil/student to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.

6.4 You must at all times conduct your computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Uses that are considered unacceptable include the following:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual-preference, or gender-related slurs or jokes.
- You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
- You must not intentionally damage, disable, or otherwise harm the operation of computers.
- You must make efforts not to intentionally waste resources. Examples of resource wastage include:
- Excessive downloading of material from the Internet;
- Excessive storage of unnecessary files on the network storage areas;
- Use of computer printers to produce class sets of materials, instead of photocopiers.
- You should avoid eating or drinking around computer equipment.
- 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.

- You **must** ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) and any other media used to store data are securely stored in a locked room or cupboard when left unattended.

- Equipment taken offsite is not routinely insured by WAT. If you take any WAT computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.

7. Be familiar with WAT's IT

7.1 WAT will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled accordingly to the role of the user. You should make sure that you familiarise yourself with any software or hardware that you use. In particular, please make sure that you understand what the software is supposed to be used for and any risks. For example:

- if you use a "virtual classroom" which allows you to upload lesson plans and mock exam papers for pupils then you need to be careful that you do not accidently upload anything more confidential;

- make sure that you know how to properly use any security features contained in software. For example, some software will allow you to redact documents (i.e. "black out" text so that it cannot be read by the recipient). Make sure that you can use this software correctly so that the recipient of the document cannot "undo" the redactions; and

- you need to be extra careful where you store information containing Critical School Personal Data. For example, safeguarding information should not ordinarily be saved on a shared computer drive accessible to all staff.

7.2 You should contact your IT Support Team for any specific guidance on the information security requirements of the different programs that are be used.

7.3 A lot of data protection breaches happen as a result of basic mistakes being made when using IT system. The following sections outline some tips on how to avoid common problems:

8. Hardware and software not provided by WAT

8.1 Staff must not use, download or install any software, app, programme, or service without permission from the IT Support Team. Staff 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.

9. Cloud storage

9.1 WAT has a set of procedures for the automatic backing up, accessing and restoring 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 it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

9.2 You must not use private cloud storage or file sharing accounts to store or share WAT documents.

10. Passwords

10.1 You will be provided with a personal account for accessing the computer system and software on there, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, **you must not disclose your password to anyone**, including IT support staff. If you do so you **must** change your password immediately.

- **Passwords should be long**, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else.

- **Your password should be difficult to guess**, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

- **You must not use a password which is used for another account**. For example, you must not use your password for your private email address or online services for any WAT account.

- **Passwords (and any other security credential you are issued with 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 or shared and should be changed regularly.**

11. Computer screens

11.1 When leaving a computer unattended, even if you are only away from the computer for a short period of time you must ensure you have either logged off your account, or locked the computer to prevent anyone using your account in your absence. To lock your computer screen press the "Windows" key followed by the "L" key. WAT's computers will be configured to automatically lock if not used within a short period of time.

12. Email (and Faxes)

12.1 All members of staff with a computer account are provided with a professional email address for communication both internally and with other email users outside the school. When sending emails or faxes you must take care to make sure that the recipients are correct.

12.2 If the email or fax contains Critical School Personal Data then you should ask another member of staff to double check that you have entered the email address / fax number correctly before pressing send.

12.3 If a fax contains Critical School Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

12.4 **You must not use a private email address for WAT related work**. You must only use your windsoracademytrust.org.uk email address. Please note that this rule applies to all employees as well as LAB members and Trustees. Please contact a member of the IT Support Team if you require an email account to be set up for you.

12.5 **Emails to multiple recipients**: You must ensure that emails sent to multi recipients do not identify other recipients and are sent securely e.g. by using special software / information management systems with clear protocol on who can send out those emails. Caution should be exercised when using blind copying (bcc) emails as there is a risk that staff could mistakenly put the email addresses in the cc field rather than the bcc.

12.6 **Remember to encrypt i**nternal and external emails which contain Critical School Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. To use encryption then you need to seek advice from the IT Support Team who will explain how to do this. If you need to give someone the "password" or "key" to unlock an encrypted email or document then this should be provided via a different means. For example, after emailing the encrypted file, the password should be shared via a telephone conversation.

12.7 There are a number of considerations when communicating by email:

- All E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may

therefore have to be made available to third parties. You must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.

- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You must not purchase goods or services on behalf of the trust via e-mail without proper authorisation.

- All e-mail you send should contain your name, job title and details of your academy and WAT.

- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material, business intelligence, trade secrets, or other confidential information belonging to WAT.

- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. WAT will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.

- You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

- You must not transmit any sensitive or personal information about staff or students/pupils via email without the data being encrypted by a method approved by WAT.

- If communicating with a student/pupil via email, always use your professional WAT account.

13. Public Wi-Fi:

13.1 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.

14. Portable Media Devices

14.1 The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices have been given to you by WAT and you have received training on how to use those devices securely. The IT Support Team will protect any portable media device given to you with encryption. Any devices that have not been encrypted must not be used for any personal or confidential data.

14.2 You **must not** store any sensitive or personal information about staff or pupils/ students on any 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.

14.3 If you find a USB stick, please pass to an IT Support Team immediately. Do not plug into a computer.

15. Using Trust laptops, phones, cameras and other devices

15.1 If you need to book out a WAT device then contact your IT Support Team.

16. Using personal devices for WAT work

16.1 You may only use your personal device (such as your laptop or smartphone) for WAT work if you have been given permission. Private equipment **must not** be used to store personal data.

16.2 Even if you have been given permission to do so, then before using your own device for WAT work you must speak to your IT Support Team so that they can configure your device as required.

16.3 **Using your own PC or Laptop:** If you use your laptop or PC for WAT work then you must use any appropriate remote access software provided by WAT. Accessing WAT's own network is far more secure and significantly reduces the risk of a security breach.

16.4 **Using your own smartphone or handheld:** Before you use your own smartphone or handheld for WAT work you must contact your IT Support Team to install any appropriate device management software provided by WAT which will help keep Personal Data secure and separate from private files.

16.5 The WAT central team and its academies 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, without further notice, all content on the device that has been created for WAT or on WAT's behalf or which contains Personal Data. Although we do not intend to wipe other data that is private in nature (such as private photographs or private files or emails), it may not be possible to distinguish all such information from Personal Data in all circumstances. You should therefore 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.

16.6 You must not do anything which could prevent any software installed on your computer or device by WAT from working properly. For example, you must not try and uninstall the software, or save WAT related documents to an area of your device not protected, without permission from the IT Support Team first.

16.7 Appropriate security measures should always be taken. This includes the use of firewalls and anti-virus software. Software or operating system on the device should be kept up to date.

16.8 Default passwords: If you use a personal device for WAT work which came with a default password then this password should be changed immediately. Please see section 10 for guidance on choosing a strong password.

16.9 Sending or saving documents to your personal devices: Documents containing Personal Data (including photographs and videos) should not normally be sent to or saved to personal devices, unless you have been given permission by the IT Support Team. This is because anything you save to your computer, tablet or mobile phone will not be protected by WAT's security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer. For example, if you saved a document to your laptop because you wanted to work on it over the weekend, then the document would still be on your computer hard drive even if you deleted it and emptied the recycle bin.

16.10 Friends and family: You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything WAT related on your device. For example, you should not share the login details with others and you should log out of your account once you have finished working by restarting your device. You must also make sure that your devices are not configured in a way that would allow someone else access to WAT related documents and information – if you are unsure about this then please speak to the IT Support Team.

16.11 When you stop using your device for WAT work: If you stop using your device for WAT work, for example:

- if you decide that you do not wish to use your device for WAT work; or
- if WAT withdraws permission for you to use your device; or
- if you are about to leave WAT

then, all WAT documents (including WAT emails), and any software applications provided by WAT for WAT purposes, should be removed from the device.

16.12 If this cannot be achieved remotely, you must submit the device to the IT Support Team for wiping and software removal. You must provide all necessary co-operation and assistance to the IT Support Team in relation to this process.

17. Portable media devices: Disposal of Trust IT equipment: WAT IT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to the IT Support Team even if you think that it is broken and will no longer work.

18. Personal Use

18.1 WAT recognises that occasional personal use of computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use;

- **must** comply with all other conditions of this policy and the Data Protection Policy apply to non-personal use, and all other policies regarding staff conduct;
- **must not** interfere in any way with your other duties or those of any other member of staff;
- **must not** have any undue effect on the performance of the computer system; and
- **must not** be for any commercial purpose or gain unless explicitly authorised by the trust.

18.2 Be aware that WAT computer systems are monitored at all times including files and emails held on WAT systems. Personal use is permitted at the discretion of WAT and access can be limited or revoked at any time. Regard should also be made to other WAT Policies including:

- Child Protection and Safeguarding Policy
- E-Safety Policy
- Social Media Policy
- Staff Code of Conduct

19. Use of your own Equipment

19.1 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.

19.2 You must not connect personal computer equipment to a WAT computer equipment without prior approval from IT staff, with the exception of storage devices such as USB memory sticks.

20. Paper files

20.1 **Keep under lock and key:** Staff must ensure that papers which contain Personal Data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

20.2 If the papers contain Critical School Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below. Information must not be stored in any other location.

20.3 **Disposal:** Paper records containing all Personal Data should be disposed of securely in accordance with WAT's Information and Records Retention Policy by placing them in confidential waste bins stored in a secure location or by ensuring that all documented has been shredded and disposed of securely. Documents containing Personal Data should never be placed in the general waste.

20.4 **Printing:** When printing documents, secure print should be set until you are ready to release the documents. Make sure that you collect everything from the printer straight away; otherwise there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains Personal Data then you must hand it in to the HR lead, the DPL or the DPO.

20.5 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed. Personal cabinets should not be used to store documents containing Critical School Personal Data. Please see paragraph 20.2 above for details of where Critical School Personal Data should be kept.

20.6 **Post:** You also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something in the post that is confidential, consider asking your IT Support Team to put in on an encrypted memory stick or arrange for it to be sent by courier.

21. Working off site (e.g. Academy trips and homeworking)

21.1 You might need to take Personal Data off site for various reasons, for example because you are working from home or supervising an academy trip. This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

21.2 Critical Personal School Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary, for example, where necessary for academy trips.

21.3 For academy trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. You must make sure that Personal Data taken off site is returned to the Academy.

21.4 If you are allowed to work from home then check with your HR lead, DPL/DPO and the IT Support Team what additional arrangements are in place. This might involve installing software on your home computer or smartphone please see the following sections.

21.5 Not all staff are allowed to work from home. If in doubt, speak to your HR lead and or your line manager.

21.6 Take the minimum with you: When working away from the Academy or WAT office, you must only take the minimum amount of information with you. For example, a teacher organising a field trip might need to take with them information about pupil/student medical conditions (for example 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.

21.7 Working on the move: You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop on a train, you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.

21.8 Paper records: If you need to take hard copy (i.e. paper) records with you then you should make sure that they are kept secure. For example:

- 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 train you must keep the documents with you at all times and they should not be stored in luggage racks;
- if travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stationary e.g. at traffic lights;
- if you have 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 (please see paragraph 21.7 above).

22 Privacy

22.1 Use of WAT's computer systems, including your email account and storage areas provided for your use, may be subject to monitoring by WAT to ensure compliance with this policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the academy or WAT office does keep a complete record of sites visited on the Internet by both students and staff; however, usernames and passwords used on those sites are NOT monitored or recorded.

22.2 You should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).

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

23. Confidentiality and Copyright

23.1 Respect the work and ownership rights of people outside of WAT, as well as other staff or students/pupils.

23.2 You are responsible for complying with copyright law and licenses 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 (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

23.3 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, also prevent viruses and other unwanted programs onto the Trust/academy account. 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). Do not rely on the claims of suppliers, who do not have specific knowledge of WAT's systems.

23.4 As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by you during the course of your employment in any way affecting or relating to the business of WAT or capable of being used or adapted for use within WAT shall be immediately disclosed to WAT and shall to the extent permitted by law belong to and be the absolute property of WAT.

23.5 By storing or creating any personal documents or files on the WAT's computer system, you grant WAT a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way WAT sees fit.

24. Reporting Problems with the Computer System

24.1 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. To this end:

24.2 You should report any problems that need attention to a member of IT Support Team as soon as is feasible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem must be reported via the online Support Request system, via emailing IT support using user name.

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

24.4 If you have lost documents or files, you should report this as soon as possible to your Data Protection Lead, the Data Protection Officer (DPO) and CEO/Academy Headteacher. The longer a data loss problem goes unreported, the lesser the chances of your data being recoverable. Also reporting a data loss e.g. student/pupil data on a memory stick or laptop is important and may need to be investigated further. (Please see WAT's Data Breach Policy).

25. Supervision of Pupil/ Student Use

25.1 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.

25.2 Academies need to ensure that there is an Acceptable User Agreement ~~Policy~~ 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.

25.3 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.

25.4 Good teaching and learning dictates that staff check websites they recommend. Please recommend websites and guide pupils/students on internet use to minimise incidents.

25.5 When publishing or transmitting non-sensitive material outside of WAT, you must take steps to protect the identity of any pupil/student whose parents have requested this.

26. Breach of this policy

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

26.2 A member of staff who deliberately or recklessly discloses Personal Data held by WAT without proper authority is also guilty of a criminal offence and gross misconduct. This could result in dismissal.

26.3 This policy does not form part of any employee's contract of employment.

26.4 We reserve the right to change this policy at any time. Where appropriate, we will notify individuals of those changes by mail or email.

26.5 All members of staff have a duty to ensure this policy is followed. You **must** immediately inform a member of the IT Support Team, or the Academy Headteacher/CEO, of abuse of any part of the computer system. In particular, you should report;

- any websites accessible from within school that you feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, picture for example;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a student via the trust's computer system.

26.6 Reports should be made either via email or the online IT Support Request system. All reports will be treated confidentially.

Appendix 1 WAT applications

Windsor High School and Sixth Form

The purpose of this Appendix is to provide guidance to staff on how to keep information secure when using each application. This will need to be completed by listing each application (e.g. software programmes, information management systems and cloud based applications) used to process Personal Data and any specific information security requirement. Software used for child protection information might require an additional level of security which may need to be explained e.g. USB keys.

Application	What it can be used for	Specific security arrangements	Any other notes / comments

Appendix 2

PCI Compliance Policy

Policy Statement

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.

Specific Policy Requirements

Network Security

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 Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

Cardholder Data

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.

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

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

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.).

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.

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 e-mail, which they suspect may contain virus.

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.

Appendix 3

Impact Levels and protective marking

- Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to academies?
Not Protectively Marked	0	Will apply in academies
Protect	1 or 2	
Restricted	3	
Confidential	4	Will not apply in academies
Highly Confidential	5	
Top Secret	6	

- Most student / pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.
- WAT will ensure that all staff, contractors and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.
- Unmarked material is considered “unclassified". The term “UNCLASSIFIED" or “NON” or “NOT PROTECTIVELY MARKED" may be used to indicate positively that a protective marking is not needed.

- All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

- Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to a person's reputation has a higher impact than damage that might cause short-term embarrassment.

- Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	The technology	Notes on Protect Marking (Impact Level)
Academy life and events	Academy terms, holidays, training days, the curriculum, extra-curriculum activities, events, displays of student's/pupil's work, lunchtime menus, extended services, parent consultation events.	Common practice is to use publically accessible technology such as academy websites or portal, emailed newsletters, subscription text services	Most of the information will fall into the NOT PROTECTIVELY (Impact LEVEL 0) category
Learning and Achievement	Individual pupil / student academic, social and Behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically academies will make information available by parents logging on to a system that provides them with appropriately secure access such as Learning Platform or portal, or by communication to a personal device or email account belonging to the parent	Most of this information will fall into the PROTECT (impact Level 2) category. There may be students/pupils whose personal data requires a RESTRICTED marking (Impact level3) or higher. For example, the home address of a child at risk. In this case, WAT may decide not to make this student/pupil record available in this way
Messages and alerts	Attendance, behavioural, achievement, sickness, academy closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by academies to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact level1) category. However, since it is not practical to encrypt email or text messages to parents, academies should not send detailed personally identifiable information. General, anonymous alerts about academy closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact level 0) Category.