

Walsall Academy



IT Security Policy & Procedures

Policy Title	IT Security Policy and Procedures
Policy Reference	WA/ITSec
Description	This document sets out the policy regarding IT security
Status	Statutory
Category	Academy
Person Responsible	M Khan – Manager of IT
Version	V 1.5 November 2025
Other relevant policies	
Adopted by the Governing Board on	
Next Review Due	November 2026
Data Protection	<i>Data will be processed in line with the requirements and protections set out in the General Data Protection Regulation</i>

Version Records		
Version	Date	Description
1.1	November 2020	Review
1.2	November 2021	Review
1.3	January 2023	Review
1.4	September 2024	Review
1.5	November 2025	Review
1.6		
1.7		

ACCESS TO WALSALL ACADEMY INFORMATION

- All information held on the IT network including email, file systems and databases are the property of Walsall Academy and staff should have no expectation of privacy for this data.
- Although it is not the general practice of Walsall Academy to monitor staff stored files, email messages and Internet access for their general content, Walsall Academy reserves the right to do so for the protection of staff, for system performance, maintenance, auditing, security or investigative functions (including evidence of unlawful activity or breaches to Walsall Academy policy) and to protect itself from potential liability.
- All student access to internal and external systems is actively monitored.
- Requests to access the computer account of a member of staff must be directed to the Manager of IT in writing by the Relevant Member of SLT via a change request system. The Manager of IT will seek the permission of the Headteacher. Where this access is granted it must be used for enquiry purposes only.
- Staff must not issue any information to third parties unless they have authorisation to do so.
- Users are only permitted to access electronic information and data that they require to perform their duties.
- There is a distinction between sensitive information and other data stored on the Academy network. Sensitive would typically mean personal or financial information. No sensitive information should be stored on any mobile devices unless the device has 256-bit AES encryption applied to it, and then only with the permission of the Manager of IT.
- If sensitive information is lost, either through loss of a laptop, computer, backup media or other security breach, the Manager of IT must be notified immediately.
- All computers must be logged off at the end of the day. This action erases residual information contained in the computer's memory and assists with overnight anti-virus software updates and automated maintenance tasks.

Data Protection Act 2018

- The Data Protection Act (2018) imposes responsibilities on users regarding the processing of personal data. Personal data refers to data relating to a living individual who can be identified either from the data, or from the data in conjunction with other information held by an organisation. It is the responsibility of all Walsall Academy staff to ensure that the principles of the Act, including all GDPR requirements, are complied with.

A summary of other relevant UK legislation is included in Appendix 1.

Personal use of computer systems

- Walsall Academy's IT based systems are provided for Academy use only.
- Staff must not use Walsall Academy's systems or the Internet for activities that are not related to the business of Walsall Academy.

PC, LAPTOP AND MOBILE SECURITY

General

- PCs and laptop computers must not be left unattended for long periods while logged in e.g. during lunch, breakfast breaks etc. Users must either logoff or lock the PC under these circumstances.
- IT equipment must not be removed from Walsall Academy's premises unless written approval has been received from the Manager of IT. All IT equipment must be signed for before being removed from Walsall Academy premises.

Software

- Software must not be copied, removed or transferred to any third party or non-Academy equipment such as home PCs without written authorisation from the Headteacher.
- Only software that has been authorised by the IT Department may be used on PCs and laptop computers connected to the Walsall Academy IT network.
- Downloading of any executable files (.exe) or software from the Internet is forbidden without written authorisation from the IT Department.
- Regular reviews of desktop software are undertaken and the presence of unauthorised software will be investigated. Walsall Academy reserves the right to remove any files or data from IT systems including any information it views as offensive or illegal.

Protection of Sensitive Information

- All Academy data held on mobile computer devices or media (e.g. CDROM, DVD, USB device, laptop, smart mobile devices etc.) must be subject to whole disk encryption.

Mobile Devices

- All reasonable precautions must be taken to protect equipment against damage, loss and theft. The equipment must not be left unattended in any public place. Damage, loss or theft must be immediately reported to the IT help desk.
- Walsall Academy's mobile devices are protected by one or more of the following systems:- BIOS passwords, OS passwords, application level passwords and 256-bit AES encryption. These must not be disabled.
- Anti-virus software is installed on all laptops and computers.
- Data must be backed-up to the Academy's network or designated cloud-based systems on a regular basis.
- Smart devices must be set with a pin number and/or biometric access and must not be used to store sensitive information.
- Mobile devices must be stored securely when not in use. Staff must not leave a mobile device unattended at any time when not secured.

Computer Viruses / Malware / Ransomware

- Corruption data or software by malicious software (e.g. a computer virus, malware or ransomware) must be reported to the IT Help Desk.
- Users are not permitted to disable or remove antivirus software or other security related software under any circumstances.

INTERNET AND EMAIL

General

- All users have a responsibility to use the Internet in a professional, ethical and lawful manner. Users must regard Internet access as a privilege, which can be revoked.
- All IT related Hardware will be disposed of safely and legally at appropriately licensed facilities, in line with the WEEE directive which became Law in 2007 and the EUGDPR covered by the Data Protection Act 2018.
- Users should exercise caution when making payments over the Internet, as the security of credit card details cannot be guaranteed. Walsall Academy will accept no liability for losses arising through the transmission of personal or financial information (e.g. credit card numbers) over the Internet.
- Users must not use Walsall Academy's Internet facilities to download, display, generate and/or pass on to others material whether in text, pictures or any other form, which would be regarded as offensive. It is important to note that what constitutes offensive material is not one for the sender to determine - it is the effect

on anyone viewing the material that is considered important. In law, possession of some material is deemed to be a serious criminal offence, whether in the workplace or otherwise.

- All access to the Internet from Walsall Academy's network will be via an approved channel that will be secured by a firewall and an appropriately configured web filter.
- Users must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, failing to exit from websites, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-educational-related uses of the Internet.
- Users must not use the same passwords for login to Internet websites as they do internally for Walsall Academy systems.
- Walsall Academy reserves the right to review, audit, intercept, access and disclose all access to the Internet. This includes emails sent and received in addition to websites visited and files downloaded from the Internet.
- At this time, access to SNS (Social Networking Sites) from within the Academy is blocked for Staff and Students. Staff have, and will continue to receive, relevant training in the use of SNS sites (from outside the Academy) in order to protect both themselves and their students. Training Materials can be found on the Staff intranet under the "Staff information | Training Materials" folder.

Email

- Email users must exercise caution with any external attachments or any URL links other than those received from a trusted source, as these attachments may contain or trigger computer virus/malware/ransomware etc.
- Users must not represent themselves as another individual in electronic communications.
- Email users must be aware of the risks associated using email to send confidential or commercially sensitive information. If such information must be sent files must be encrypted with a password and should be sent separately using a different method where possible.
- Users must ensure that documents attached to emails are not copyright protected.
- Email messages must be appropriate and professional.
- As email is a form of publishing and covered by relevant publishing Acts, libellous and defamatory material is not permitted.

- Users should be aware of their obligations under the Data Protection Act 2018 and must not use email for transmitting data of a personal nature related to a third party.
- If any person receives email, which they deem to be inappropriate, offensive or illegal, they must inform the "Relevant member of SLT". Immediate reporting of incidents facilitates more successful identification of the source and other details.
- All emails that are sent externally must carry a standard Walsall Academy disclaimer. Users must not attach their own disclaimers to emails.
- From time to time the IT department will send test phishing emails out to staff. The purpose of this would be to increase the awareness of potential cyber threats. If a staff member does not successfully detect these emails, they would be required to complete a short training guide to help develop their security awareness.

UNSOLICITED COMMUNICATIONS - Email

- Software is in place to monitor incoming and outgoing external email messages. Messages that contain text which indicate that they may have come from an unsolicited source are 'quarantined' by the software and an automatic email is sent to the Walsall Academy sender or recipient to inform them that a message has been stopped. Please contact the IT Help Desk if you receive a quarantine message.

TELECOMMUNICATIONS – Remote Access

- Remote Access can be defined as "Access to Walsall Academy's IT resources or data from a location external to Walsall Academy". This access may be by a third party or an employee who is located off-site.
- Access to Walsall Academy's internal systems for staff, students and parents is only available via the publicised secure communications gateway accessible via the Walsall Academy website.

THIRD PARTY ACCESS

- Third Party Access can be defined as "The granting of access to Walsall Academy's IT resources or data to an individual who is not a student, parent of a current student or employee of Walsall Academy".

Examples of third parties include:

- Software vendor who is providing technical support;
- Contractor or consultant;
- Service provider; and
- An individual providing outsourced services to Walsall Academy requiring access to applications or data.

- Third Party Access can only be provided after the third party has signed a confidentiality agreement that must be included in their formal contract with Walsall Academy. Walsall Academy staff must never permit another individual to utilise their user name to access the Walsall Academy network.
- Further requirements for granting Third Party Access are:
 - Risk analysis process
 - Approval by Data Owner
 - Approval by the Manager of IT
- Third party access will only be permitted to facilities and data which are required to perform specific agreed tasks as identified by Walsall Academy.

SOFTWARE LICENCES – Copyright

- Copyright stipulations governing vendor-supplied software must be observed at all times.
- The IT Department is responsible for maintaining records of software licences other than those which are curriculum specific, in which case the curriculum areas nominated user will be responsible. Software that is acquired on a trial basis must be used in accordance with the vendor's copyright instructions.
- All software developed within Walsall Academy is the property of Walsall Academy and must not be copied or distributed without prior written authorisation from the Academy.

DATA BACKUPS

- The IT Department must take regular daily backups of all the Academy's internal and cloud-based IT systems.
- Users must always save data and files either on the Academy internal network drives or within the Academy Microsoft OneDrive and SharePoint environment as opposed to any local media e.g. USB memory sticks. This ensures that regular backups are taken and are available for recovery purposes. Users should be aware that data saved on any other media is not backed up by the IT Department.

Appendix 1

Legislation

The following is a list of UK legal acts and ISO standards that relate to the use of IT systems:

- Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation (GDPR))
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- ISO 27001 Security Management Standard

This list should not be seen as all-inclusive.

It is the responsibility of Walsall Academy staff to make themselves aware of their obligations under UK law as it relates to the use of IT.

This Policy is not exclusive and should be read in conjunction with other related Academy policies including, but not limited to those listed below:

- Data protection policy
- IT Acceptable use policy
- CCTV Policy
- eSafety Policy
- BYOD Policy