Pendle
Education Trust

Policy/Procedure/Guideline Review

Policy/Procedure/Guideline:	Acceptable use of ITL systems and resources Policy
Senior Manager Responsible:	Executive Director for ITL
JCNC Consultation:	December 2021
Trust Approval:	13 December 2021
Review date:	December 2024

Contents

1. Overview

Pendle Education Trust (Trust) wishes to encourage the use of its Information Technology for Learning (ITL) facilities, subject to adherence to its policies, and is committed to protecting its staff, students, partners and the Trust from illegal or damaging actions by individuals, either knowingly or unknowingly.

The Trust ITL facilities, including computer equipment, software, operating systems, storage media, networks, web browsing, email and file transfer, are the property of the Trust. These facilities are to be used in the interests of the Trust, and of our staff and students, in the course of normal operations.

Legislation exists that defines the limits and acceptable use of computer systems and information. Compliance with this policy should ensure that legal requirements are observed. Effective security requires the participation and support of all staff, students and others who deal with information and systems. It is the responsibility of every user to know this policy and guidelines, and to use the Trust ITL facilities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable and safe use the Trust IT facilities, to protect staff, students and the Trust. Inappropriate use exposes the Trust to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This Policy applies to all staff and students at the Trust, as well as visitors, contractors and others using any computer equipment, software and systems that are owned or leased by the Trust.

4. Related Policies

	Local Academy Level Policy	Trust Policy
Online Safety and Cyber Bullying policies, which may be stand-alone policies or incorporated within the academy Safeguarding and Child Protection Policy and/or Behaviour Policy	X	
Academy policy students use of devices, which may be included in the academy's student code of conduct, Teaching and Learning Policy, Behaviour Policy and/or other relevant policies	X	
Online Safety education and Computing education, included within the academy Curriculum and/or RSHE policies	X	
Code of Conduct for Parents and Home-Academy agreements	X	X
GDPR Policy		X
Social Media Policy		X
Staff Code of Conduct		X
Financial Policies and Procedures and Financial Regulations		X
Risk Management Policy		X
Critical Incident Plans	X	
Managing Discipline Procedure		X

See also relevant legislation (Appendix A)

5. Roles and Responsibilities

PET ITL Team

Executive Director for ITL: is responsible for the creation and review of this policy, monitoring its effectiveness and suitability, and ensuring and monitoring its implementation.

ITL Team Leader: is responsible for implementation of the policy across the Trust's ITL resources and ensuring ITL systems and processes are designed to meet all legal and policy requirements.

The ITL Team: are responsible for:

- maintaining the Trust's network and systems security, so that it is meeting cyber safety technical requirements,
- ensuring staff and secondary age student users may only access networks and devices through properly enforced password protection policy, and appropriate levels of access are in place for primary age students,
- ensuring user access rights are set appropriately for each member of staff, as authorised by the Principal within each Academy and/or the Executive Director for ITL,
- the internet filtering policy is applied and updated on a regular basis, and that the use of the network, internet and Trust devices are regularly monitored in order that the relevant members of staff in each academy are alerted to any suspicious searches or breaches,
- that they keep up to date with cyber security technical information in order to effectively carry out their role and to inform and update others as relevant.

Principal and Senior Leadership Team, including DSL and/or Online Safety Lead in each academy

Principal and Senior Leadership Team: are responsible for:

- ensuring staff within the academy adhere to the Trust Policy, ensuring staff are aware of the contents of the policy and sign and adhere to the staff Acceptable Use Agreement (Appendix B), and for taking action in line with the Trust Managing Discipline Procedure if required.
- determining the appropriate access rights for the network and any programmes/apps used by the academy for each member of staff and working with the ITL team to ensure these are set correctly,
- ensuring that any associated policies are written in line with this policy.
- the education of students in how to keep themselves safe online and the responsible use of the internet and digital devices, including ensuring students (or parents for younger students) sign and adhere to the student Acceptable Use Agreement (Appendix C), and for taking action in line with the Academy Behaviour and/or Safeguarding policy if required.
- ensuring that the DSL and/or Online Safety Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as required.

DSL and/or Online Safety Lead: in addition to the role of the Senior Leadership Team, are responsible for academy level monitoring of student's internet use, taking appropriate action on any suspicious searches or breaches.

Core Trust and Academy Staff

All staff: are responsible for:

- ensuring they have an up-to-date awareness of cyber safety matters and of the Trust and Academy online safety policy and practices.
- they have read, understood and signed the staff acceptable use agreement (Appendix B).
- they monitor the use of online access and digital devices by students, reporting any suspected misuse or problem to DSL/Online Safety Leader in the relevant Academy.
- ensuring all digital communications with students and/or parents/carers should be on a professional level and only carried out using official Academy/Trust systems.
- ensuring that any visitors making use of Academy/Trust devices or internet access have signed and agreed to the visitor acceptable use agreement (Appendix D); and that they are provided with information about how and when they are permitted to use mobile technology and the ITL network.
- reporting any damage or technical issues to the ITL team for repair and maintenance.
- ensuring the safe keeping of personal data, minimising the risk of its loss or misuse. This includes being alert to a possible breach, understand the need for urgency and know who the Data Protection Officer is to report it to within the Academy.

Students and Parents

Students: Students are responsible for, at an age-appropriate level:

- using the Academy/Trust ITL systems in accordance with Student Acceptable Use Agreement (Appendix C) and other Academy policies, including keeping their individual user accounts secure and not allowing others to access them.
- understanding the need to avoid plagiarism and uphold copyright regulations.
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- understanding the importance of adopting good online safety practice when using digital technologies and realise that the Academy's policies cover their actions outside of school, if related to their membership of the Academy/Trust.

The Academy/Trust will ensure students are:

- taught about online safety issues, such as the risks attached to the sharing of personal details,
- strategies to deal with inappropriate communications
- and of the need to communicate appropriately when using digital technologies.

Parents: Parents/carers should follow the Academy/Trust Code of Conduct for Parents, which includes online activity and use of social media.

Parents should support their child with complying with Student Acceptable Use Agreement (Appendix C), especially with younger children who are not able to take responsibility for that agreement independently. Parents/carers play a crucial role in ensuring that their children

understand the need to use the internet/mobile devices in an appropriate way. Parents and carers will be encouraged to support the Academy/Trust in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy/Trust events.
- access to parents' sections of the website and (where used) digital learning portfolios.
- Academy/Trust devices loaned to their children and their children's personal devices at home.

The Academy/Trust will support parents/carers by providing information and awareness of online safety through the Academy website, as well as in letters, newsletters, email and text messages.

Trust Board and Local Governing Committee of each academy

Trust Board: responsible for the approval this Acceptable Use of Information Technology for Learning (ITL) policy.

Local Governing Committees: responsible for the approval of associated policies and reviewing their effectiveness. These include all policies covering education of students on online safety, cyber bullying and use of devices.

6. ITL facilities and resources - Policy Statement

Use of ITL facilities and resources is permitted for legitimate purposes and is subject to authorisation. Legitimate purposes include legal use in connection with teaching, learning, research and approved business activities of the Trust by its staff, students and other authorised persons, including the recognised trade unions in order that they may communicate with their respective memberships.

The Trust reserves the right to monitor and record transmissions made through its IT facilities to ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Telecommunications) 2000 Regulations.

6.1. Device, Network and Internet Access

User access levels and the use of passwords

The ITL Team will ensure user access rights are set appropriately for each member of staff, as authorised by the Principal within each Academy and/or the Executive Director for ITL. The ability to access an ITL facility does not imply a right to use that facility or access data. All staff, student and visitor users should only have access to what they require for their role. Under no circumstances should personal or other confidential information held on computer be disclosed to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

If users have any doubts about which facilities they are authorised to access they should seek clarification from an appropriate member of staff. All users are responsible for reporting any additional access for themselves or others to systems or data that they do or do not require with the ITL Team so this can be amended, this includes where staff have changed job roles.

All network devices and systems require a password. Passwords protect Trust systems from access by unauthorised people. They protect users work and the Academy's or Trust's

information. Therefore, a user's individual password(s) should never be disclosed to anyone else, and users must not share access to their individual accounts. Authorised users are responsible for the security of their passwords and accounts and will be held responsible for all actions performed by use of their User ID. Users must ensure that their unattended workstations or devices are secure, locking them if they are away from their workstation/device so no one is able to use their accounts without their knowledge.

Some Primary aged student users may access the Academy/Trust network using group usernames and passwords as set by the Primary Academy. Where this is the case, best practice is for students to regularly use an allocated device. The Academy/Trust uses static IP addresses for mobile devices, allowing an incident to be traced to a given device and therefore a specific user if devices have been allocated appropriately by staff. Teachers and Teaching Assistants are responsible for closely monitoring students when using any digital/online device.

The ITL Team follow guidance from the National Cyber Security Centre that passwords should not be set to expire, passwords are of a minimum length, complexity and old passwords cannot be reused immediately. If there are any concerns about passwords being known, this must be reported to the ITL Team so that action can be taken ensuring only the intended user is able to reset and know the new password. If this security breach may have enabled access to data, the Data Protection lead must also be notified.

The administrator passwords for the academy systems, will be known by the ITL Team and will only be shared with the Principal/SLT and Online Safety Leader within each Academy as required.

The Trust reserves the right to limit or restrict any user's access at any time.

Network Infrastructure security

The ITL Team is to be responsible for ensuring that the Academy/Trust infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Academy/Trust technical systems will be managed in ways that ensure that the Academy/Trust meets recommended technical requirements.
The Trust does not allow the connection of non-corporate computer equipment to the network without prior technical approval. This includes connection via dialup or Virtual Private Networking (VPN).

Servers, wireless systems, and cabling must be securely located and physical access restricted. The physical locations of all core network equipment are secured with access means to ensure only the ITL team, Site staff and Senior Leadership Team have access. Each entrance to a server room will be recorded with a name and signature, and 3rd parties accompanied whilst working in these locations. Each site will have appropriate measures in place for access to the building such as an alarm system & CCTV.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the Academy/Trust systems and data. These are tested regularly. The Academy/Trust infrastructure and individual devices are protected by up-to-date virus software.

Pro-active monitoring is in place via the ITL team & a 3rd party support team to help protect the Academy/Trust infrastructure and digital data – this includes emergency patching for known security issues.

Internet Access – filtering, monitoring and anti-virus

Internet access is filtered for all users. The Trust provides enhanced/differentiated user-level filtering (allowing different filtering levels for staff, visitor and student users).

Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

The ITL Team, as well as DSLs/Online Safety Leaders in each Academy, regularly monitor and record the activity of users on the Academy/Trust technical systems and users are made aware of this in the acceptable use agreement.

Staff users must report any actual/potential technical incident/security breach to the ITL Team, in some cases this may be via the DSL/Online Safety Leader. Reports from student users are made to the class teacher to report.

Anti-virus software is loaded on all computers as standard and is updated regularly via the network. Antivirus software must not be de-installed or deactivated. Files received by or sent by email are checked for viruses automatically. Staff using their own equipment are responsible for maintaining up to date virus definitions on their computers and can contact The ITL Team for help as required. Users must not intentionally access or transmit computer viruses or similar software. Non-Trust software or data files intended to be run on Academy/Trust equipment by external contacts such as engineers or trainers must be checked for viruses before use. If it is suspected that a virus has infected a computer/device, then stop using the computer/device and contact The ITL Team immediately.

6.2. Mobile Technologies

Mobile technology devices may be Academy/Trust owned/provided or personally owned and might include smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the Academy/Trust's WiFi network. The device then has access to the wider internet, which may include other cloud-based services such as email and data storage.

Unlike fixed devices which are able to be connected to the network through hardware, mobile devices will be connected to the Academy/Trust's WiFi network. The Trust has provided technical solutions for the safe use of mobile technology for both Academy/Trust and personal devices:

- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g., Internet only access, network access allowed, shared folder network access).

- Filtering will be applied to the internet connection and attempts to bypass this are not permitted.

- All Academy/Trust devices and the use of Academy WiFi are subject to routine monitoring.

Use of Academy/Trust and personal mobile devices within the Academy/Trust
Academy/Trust mobile devices used within our Academies should be treated the same as fixed devices/equipment, with responsible use and management of these resources and reporting of any issues to the ITL team.

Staff can make full use of their Academy/Trust devices within our academies, including where they are visiting a different academy to their main place of work. The Staff Acceptable Use

Agreement applies across the Trust. The Staff Acceptable Use Agreement allows restricted use of personal mobile technologies on the premises and use of Academy WiFi even on personal devices is subject to the same Staff Acceptable Use Agreement and requirements of this policy.

The Visitor Acceptable Use Agreement allows restricted use of personal mobile technologies on the premises. Visitors may be provided with the WiFi password for use on personal devices in circumstances agreed by the Principal, member of SLT or Online Safety Leader. This will be upon the signing of the Visitor Acceptable Use Agreement.

Students are not permitted to access to the academy's wireless network via personal digital devices.

Personal devices are brought into the academy entirely at the risk of the owner and the decision to bring the device in lies with the user, as does the liability for any loss or damage resulting from the use of the device. The Academy/Trust accepts no responsibility or liability in respect of lost, stolen or damaged devices while on the premises or on activities organised or undertaken by the Academy/Trust (the Academy/Trust recommends insurance is purchased to cover the device whilst out of the home). The Academy/Trust accepts no responsibility for any malfunction of a device due to changes made to the device while on the academy network or whilst resolving any connectivity issues.

Users are responsible for keeping their personal device up to date through software, security and app updates. They should ensure their device is virus protected and should not be capable of passing on infections to the network. Equipment authorised for connection must undergo portable appliance testing (PAT), if appropriate, prior to connection, at the expense of the user. Access to the ITL network will be denied if the ITL team are concerned of any of these requirements not being followed.

If any personal equipment authorised for connection to the Trust's ITL facilities is suspected of causing degradation to the performance of any Trust ITL facility, the Trust reserves the right to remove it immediately without notification to the owner. The Trust disclaims any responsibility for any damage occurring to personal equipment connected to Trust ITL facilities, whether authorised or unauthorised, during connection to or removal from the Trust's ITL facilities.

The Academy/Trust has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate while on the ITL network.

Use of Academy/Trust mobile devices outside of the Academy/Trust

Staff may use Academy/Trust provided equipment at home. This is subject to the staff Acceptable Use Agreement and requirements of this policy. Devices will be enabled for use outside of the Academy/Trust network, to connect to home/other WiFi. Staff are expected to keep these devices secure and not allow access to any confidential, personal or sensitive information by anyone outside of the Trust.

Students may use Academy/Trust provided equipment at home, is subject to the student Acceptable Use Agreement (Appendix C), requirements of this policy and the home-academy loan agreement (Appendix E). Devices will be enabled for use outside of the Academy/Trust network, to connect to home/other WiFi. Students are expected to use these devices for educational purposes. Safeguarding and security software will be installed to monitor and restrict access to inappropriate content online. Devices loaned to students for home use can be recalled at any time.

Academy/Trust resources used off site, including at home, remain under Academy/Trust warranty and/or insurance. The Trust accepts liability for any loss or damage caused as a result of an accident. Any loss or damage as a result of deliberate, malicious or reclass use may result in action in line with the Managing Discipline Procedures for staff or Academy Behaviour Policy for students. Associated costs may also be reclaimed from staff and students if appropriate.

Accessing Academy/Trust ITL facilities on personal devices
Use of personal devices to access ITL facilities, for example having email or Teams apps set up on a personal mobile, is permitted but users should ensure Passcodes or PINs are set to aid security. Use of these systems are subject to the same Acceptable Use Agreements and this policy.

The ITL Team can offer advice but will not install, set up or alter any settings on a personal device. The Trust is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

The Trust respects the work-life balance of all our staff. It is the user's choice to access Academy/Trust systems on a personal device and is not required by the Trust. Users are recommended to use device settings to only receive communications through these facilities during the users' working hours.

6.3. Software, including apps and web-based programmes

Installation and maintenance

Installation of new software, apps and web-based programmes must be arranged through the ITL Team. Only software properly purchased and approved through the ITL Team may be used on Academy/Trust hardware.

The software and apps originally installed by the ITL Team must remain on the Academy/Trust owned device in usable condition and be easily accessible at all times. The Academy/Trust may add software applications at any time. Periodic checks of devices are made to ensure that users have not removed required apps. The ITL Team will ensure that all Academy/Trust devices contain the necessary software and apps for the users who use that device.

The Trust reserves the right to inspect copy, remove or otherwise alter any data, file, software or system that may undermine the integrity or authorised use of that facility with or without notice to the user.

Licences
The ITL Team is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

It is the responsibility of the individual requesting the software, app or web-based programme to ensure that any licensing issues are addressed promptly, either by on-line registration or the purchasing of a valid licence(s) through the ITL Team as part of the installation request.

The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licences must always be adhered to. Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which

contravenes the licensing regulations above must report this to the ITL Team to resolve any issues including removing the programme if required.

Individual user accounts and/or MIS integration/extraction

The ITL Team will carry out a GDPR Supplier Assessment (Appendix F) for all software, apps or web-based programmes which involve an individual user account or MIS integration/extraction will have access to personal data. This will be done when requests for new suppliers are made by staff, and their request has been approved by a member of the relevant Academy's SLT. The GDPR Supplier Assessment must be completed, and the supplier approved by the Executive Director for ITL or the ITL Team Leader before accounts or MIS access are enabled. Records of approved suppliers will be kept on GDPR Sentry.

The ITL Team will carry out regular monitoring of MIS integration/extractions, ensuring that only active systems are enabled and that the data shared is limited to only what the essential information required. Our 3rd parties also ensure that should a supplier require new or amended permissions for the MIS integration/extraction that the data will stop being uploaded and will require re-authorisation by the ITL Executive Director / ITL Team Leader.

See also GDPR Policy

6.4. Email and electronic communications

The Academy/Trust email and other electronic messaging systems are provided for business purposes only, this includes but is not limited to user email addresses, chat facilities and online posts through Trust platforms such as MS Teams, and content added to shared access documents. Users should be aware that Academy/Trust email and electronic communications are monitored.

Email and online messaging are a critical business tools, but inappropriate use can expose Trust and the user to significant liability. Liability can arise in a number of ways including, among others, copyright or trademark infringement, misuse of confidential information, defamation and liability for inaccurate statements.

Email and online messages must be treated like any other formal written communication. They cannot be considered to be private, secure or temporary. They can be copied and forwarded to numerous recipients quickly and easily and it should be assumed that they could be read by anyone. Any digital communication between staff and students or parents/carers (e.g., via email, Seesaw or MS Teams) must be professional in tone and content. These communications may only take place on official Academy/Trust systems and comply with Academy communication procedures.

Improper statements in email and in online messages can give rise to personal liability and liability for the Trust and can constitute a serious disciplinary matter. Emails or online messages that embarrass misrepresent or convey an unjust or unfavourable impression of Trust or its business affairs, employees, suppliers, students or competitors, or that are defamatory, are not permitted. This includes any email or online messages that may be intimidating, hostile or offensive including on the basis of any form of discrimination.

Confidential, personal and sensitive information sent outside of the Trust must be encrypted, with passwords or access codes sent in separate communications.

Copyright law applies to email and online messages, and Academy/Trust email and online messages must not be used to transmit or circulate copyrighted materials.

Users must immediately report to the Principal, a member of SLT or the Online Safety Lead, receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, breaches or encourages a breach of copyright law; and users must not respond to any such communication.
Users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses or other damaging content. If users are unsure, they should not open the email or attachment, and must report it to the ITL Team to investigate.

6.5. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Students should understand that they must not take, use, share, publish or distribute images of others without their permission.

Consent from parents or carers will be obtained before digital images of students are published on the Academy/Trust website/social media/local press. Parental consent is obtained when a child starts at an academy and applies lasts throughout the child's time at that academy. Parents/carers have the right to withdraw consent at any time, notifying the academy of this in writing.

Staff are allowed to take digital/video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images must only be taken on Academy/Trust equipment; the personal equipment of staff must not be used for such purposes. Digital and video images must be stored in Academy/Trust network or cloud storage only. Where digital and video images are stored locally on an Academy/Trust device, the user should transfer these to network or cloud storage and ensure the local copy is deleted. This ensures that these images are kept securely and cannot be accessed if that device is lost/misplaced.

Care must be taken when taking digital/video images that students/students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy/Trust into disrepute. Photographs published on the Academy/Trust website, or elsewhere that include students/students will be selected carefully and will comply with good practice guidance on the use of such images.

Digital and video images of children will be stored for appropriate time periods following the GDPR policy. The parental consent form includes a disclaimer regarding the historical use of published images, as photos of children who have since left the Academy/Trust may remain on the Academy/Trust website and other publications including banners and promotional materials.

6.6. Data Storage and Security

Personal data will be collected, stored and processed in accordance with the General Data Protection Regulation (GDPR). Please refer to the Pendle Education Trust GDPR Policy for more information.

The Trust provides users with access to local and cloud storage for their files. These systems are managed by the ITL Team, ensuring that the Academy/Trust infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

The Trust disclaims responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of its IT facilities.

The Trust will ensure reasonable security testing of digital data and its physical location security is undertaken at regular intervals by the ITL team and 3rd party companies following guidance from The National Cyber Security Centre.

Local Data Storage and Security
It is Academy/Trust policy to store data on a network drive where it is regularly backed up. All users should only save files to their home area (My documents) and shared drives dedicated to staff or student storage, unless special arrangements have been made with the Executive Director for ITL and the ITL Team Leader.

Users should ensure that data that is stored to any other local and/or portable device, including personal devices, is regularly backed up and appropriately secured.

When any confidential, personal or sensitive data is stored locally on any mobile/portable devices:

- the data must be encrypted, and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete
- the user must keep the device secure
- the user must report any loss, damage or potential breach to the Data Protection officer and ITL team immediately.

Users have a fixed amount of storage available for their use and are expected to archive and remove data in line with GDPR regulations, if data size is impacting any ITL facilities such as backup this data may be removed or relocated to ensure continued service.

Back Ups

Backups of all Academy/Trust data are made on a regular basis and in the event of a system failure the ITL Team will attempt to restore data.

The Trust cannot guarantee that data will be restored. At the present time, there is no means for users to request that files be restored because of accidental erasure.

Visitors (non-staff or student) users are responsible for backing up their own data.

All users should be aware that any data saved anywhere other than their home area (My documents) and shared drives dedicated to staff or student storage are unlikely to be backed up unless special arrangements have been made with the Executive Director for ITL and the ITL Team Leader.

A physical copy of the Academy's data is stored locally in a secure location. This data could also be stored across the Trust's academies or agreed on secure location via the ITL Executive Director and ITL Team Leader to be used in disaster recovery scenarios.

An off-site cloud backup is also in place for disaster recovery procedures that is separate to the Academy/Trust network. See also Critical Incident and Risk Management plans.

Cloud Storage
Cloud storage is available to users through the Academy provided systems (Office 365 / Gmail). The use of cloud storage enables shared access to files through any internet connected device. Users do not need to be on the Academy/Trust network to access these files.

Any offline assess to these files should be arranged by the user, making use of the tools provided by Microsoft/Google to sync to cloud storage when back online. The ITL team can support users to set this up on any Academy/Trust devices.

The Academy provided systems (Office 365 / Gmail) have been approved, through a GDPR assessment (Appendix F), but users should be aware that the Academy/Trust does not back up this cloud storage currently. Any measures in place for back-up or restoring capabilities are via the manufacturer providing the platform (i.e., Microsoft/Google). The Trust will endeavour to put in place back-ups for cloud storage in the future.

Any cloud storage outside of Academy/Trust platforms are the responsibility of the user to ensure this data meets GDPR standards and any data must have gone through a GDPR assessment (Appendix F) via the ITL team.

6.7. Purchasing of ITL Equipment and Resources

Purchasing of ITL hardware and software will be done through the ITL Team, with authorisation from the Executive Director for ITL and ITL Team Leader, working with the Academy Principals and member of SLT. This ensures that all purchases are suitable for use on the Trust/Academy network, are managed according to Trust ITL Team procedures and that where there are opportunities to co-ordinate purchasing across the Trust this is investigated.

All ITL purchasing will comply with the PET Financial Policies and Procedures and PET Financial Regulations.

6.8. Disposal of Redundant ITL Equipment

All redundant ITL equipment will be disposed of through an authorised company, ensuring that GDPR requirements are met. Where possible this could include companies who will purchase devices for reuse, refurbishment or recycling parts. Any funds from this will be reinvested in the purchase of new ITL equipment or software. For approval companies should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. All redundant ITL equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. Only authorised companies who supply a written guarantee that this happens will be used. Disposal of any ITL equipment will conform to current relevant legislation. The ITL Team will maintain a record of disposal.

6.9. Access to and Use of Social Media

See the Trust Social Media Policy and Staff Code of Conduct

The Trust's IT Systems are first and foremost teaching and business tools, and as such personal usage of the systems is a privilege and not a right. Staff are permitted to make

reasonable and appropriate use of social media websites where this is part of the normal duties of their work and access to these will be available to staff on Trust devices.

Computers and other devices, fixed and mobile, are the property of the Trust and are primarily designed to assist in the performance of work duties. To ensure appropriate use of the internet, the Trust's internet software monitors all websites visited by staff for business and security purposes. Therefore, staff should have no expectation of privacy when it comes to the sites they access from Trust computers and devices.

At present, the Trust denies access to social networking sites to students across all our academies. Students are taught about responsible use of social media and the internet as part of online safety education. Our students are asked to report any incidents of cyber bullying to the staff in their academy.

7. Acceptable Use

In addition to this policy, the three Acceptable Use Agreements (included in the Appendix) detail the requirements for Staff, Students and Visitors. The relevant agreement needs to be signed before the user is able to access the Trust network or resources (in the case of younger students this may be signed on their behalf by parents/carers). Users are expected to act responsibly, safely and respectfully when using any Academy/Trust ITL resources or facilities, including hardware, software, web-based programmes and apps.

Whilst the Trust would like to provide a reasonable level of privacy, users should be aware that the data they create on the Trust's ITL facilities remains the property of the Trust. Confidentiality of information stored on the Trust's ITL facilities cannot be guaranteed. For security and network maintenance purposes, authorised individuals within the Trust may monitor ITL facilities at any time.

Staff and students are responsible for exercising good judgement regarding the reasonableness of personal use. If there is any uncertainty, staff should consult their manager and students their teacher. The Executive Director for ITL and the ITL Team Leader can also provide advice.

All staff are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to their line manager. This includes reporting where any accounts have been 'hacked' and therefore the content has not been accessed/added/deleted by the member of staff.

ITL equipment must be treated with care and in accordance with operating instructions. Equipment labelled as "Out of Order" must not be used. Staff should report any equipment with an apparent fault or damage to the ITL Team as soon as possible. Other users should report the fault to a member of staff as soon as possible. Equipment that is thought to be unsafe must not be used and the fault should be reported immediately to the ITL Team.

7.1. Unacceptable Use

The lists below are not exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use. The Executive Director for ITL, in agreement with Academy Principals or Executive Trust staff, may exempt designated members of staff from specified restrictions in order to permit them to undertake their legitimate job responsibilities. Under no circumstances are staff authorised to engage in any activity that is illegal while using Trust IT facilities. Incitement to commit a crime is itself a criminal offence whether or not the crime is subsequently committed. This includes the provision of information via computer

systems to facilitate crimes. Materials lawful in their place of origin may but not be lawful in the UK and vice versa.

System and Network - Prohibited Activities:

- Violation of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Trust.

- Unauthorised copying of copyrighted material including digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Trust or the end user does not have an active licence.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

- Revealing your account password to others or allowing use of your account(s) by others.

- Actively engaging in procuring or transmitting material that is inappropriate or illegal.

- Circumventing, or attempting to circumvent, user authentication or security of any system, network or account. Users should not access or try to access any user ID or data of another user or attempt to masquerade as another user.

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session or account, via any means. Disabling or restricting student user access must be done through the ITL team and in accordance with academy policies and using Trust programmes for the appropriate classroom controls.

Data Security – Prohibited Activities:

- Attempt to circumvent data protection schemes or uncover security loopholes. Any user who finds a possible security weakness on any Trust system is obliged to report it to the ITL Team. Users are also responsible for reporting any violation of this policy by another individual.

- Executing any form of network monitoring which will intercept data unless within the scope of authorised duties.

- Effecting security breaches or disruptions of any internal or external network communication. Security breaches include accessing data of which the user is not an intended recipient or logging into a server or account that the user is not authorised to access, unless these duties are within the scope of legitimate job responsibilities.

- Transmitting data through Trust systems to others who are not authorised to access that data.

Email, electronic messaging including in online documents and phone - Prohibited Activities:

- Using offensive or inappropriate terms, or any other material, which may be considered offensive and/or prejudicial to the interests or reputation of others or of the Trust.

- Creating or sending or forwarding unsolicited bulk email messages ("junk mail" or "spam"), including "chain letters", "Ponzi" or other "pyramid" schemes of any kind.
- Any form of harassment whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header or footer information.
- Any form of business activity not directly related to the work of the Trust.
- Sending confidential materials, including personal data, in an unencrypted form.

7.2. Breach of policy

Incident Reporting
Any damage/faults, security breaches, unauthorised use or suspected misuse of ITL equipment or software must be reported to the ITL team, through the helpdesk, as soon as possible.

Additionally, all security breaches or attempts; loss of equipment which would enable access to any Trust owned data; unauthorised use, sharing or access to any Trust owned data must be immediately reported to the academy's Data Protection Officer. See also the Trust's GDPR policy.

Misuse and Infringements
Violation of this policy may result in the immediate withdrawal of the user's access to Trust ITL facilities.

Any actions by a student that fails to comply with this policy will be managed using the Academy Behaviour Policy.

Any actions by a member of staff that fails to comply with this policy may result in action having to be taken by the Academy/Trust following the Managing Discipline Procedure based on the severity of the incident.
Trust wishes to promote the highest standards in relation to good practice and security in the use of information technology. Consequently, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, including any suspicion that the web site(s) or communications concerned may contain child abuse images, or if there is any other suspected illegal activity, the police will be informed, and a criminal prosecution may follow.

8. Risk Management

The ITL Team will engage with internal and external audit processes to review and evaluate the risk and security of the network and infrastructure. The ITL Team will undergo regular testing of the security of the network to identify potential risks and take action to secure the network if required. From time to time, the use of external consultants will be necessary. The use of specialist third parties for consulting and reporting can increase the reliability of the internal control systems.

The Executive Director for ITL and ITL Team Leader will plan for and mitigate against potential risks, to the ITL resources/facilities including loss of access, as part of:
- each Academy Critical Incident Plan working with the Principals in each Academy.
- the Trust Risk Management Team.

See also PET Risk Management Policy.

Appendix A – Relevant Legislation

The following are a list of Acts that apply to the use of ITL facilities. This is not an exhaustive list and represents the current legislation at the time of writing this policy. Where legislation is updated or new relevant legislation is created before the review date of this policy, this policy will be considered for earlier review as appropriate.

- Keeping Children Safe in Education 2021 - KCSIE 2021
- General Data Protection Regulations 2018 / Data Protection Act 2018 - https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- Computers' Misuse Act 1990 - https://www.legislation.gov.uk/ukpga/1990/18/contents
- Copyright, Designs and Patents Act 1988 - https://www.legislation.gov.uk/ukpga/1988/48/contents
- Communications Act 2003 - https://www.legislation.gov.uk/ukpga/2003/21/contents
- Malicious Communications Act 1988 - https://www.legislation.gov.uk/ukpga/1988/27/contents
- The Investigatory Powers (Interception by Businesses etc. For monitoring and Record-keeping Purposes) Regulations 2018 - https://www.legislation.gov.uk/uksi/2018/356/contents/made
- Investigatory Powers Act 2016 - https://www.legislation.gov.uk/ukpga/2016/25/contents
- Protection of Children Act 1978 - https://www.legislation.gov.uk/ukpga/1978/37
- Protection from Harassment Act 1997 - https://www.legislation.gov.uk/ukpga/1997/40/contents
- Equality Act 2010 - https://www.legislation.gov.uk/ukpga/2010/15/contents
- Race and Religious Hatred Act 2006 - https://www.legislation.gov.uk/ukpga/2006/1/contents
- Disability Discrimination Act 1995 - https://www.legislation.gov.uk/ukpga/1995/50/contents
- Obscene Publications Act 1959 - https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
- Criminal Justice Act 2003 - https://www.legislation.gov.uk/ukpga/2003/44/contents

- Defamation Act 2013 - https://www.legislation.gov.uk/ukpga/2013/26/contents/enacted
- Freedom of Information Act 2000 - https://www.legislation.gov.uk/ukpga/2000/36/contents
- Sexual Offences Act 2003 - https://www.legislation.gov.uk/ukpga/2003/42/contents
- Human Rights Act 1998 - https://www.legislation.gov.uk/ukpga/1998/42/contents
- Public Order Act 1986 - https://www.legislation.gov.uk/ukpga/1986/64/contents

Appendix B – Staff Acceptable Use Agreement

Pendle Education Trust – Staff ICT Acceptable Use Agreement (AUA)

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Agreement is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Pendle Education Trust and each Academy's systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The academy will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff to agree to be responsible users.

I understand that I must use academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that all students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

If you have any concerns or require clarification on the any the points below, please discuss these with the Online Safety Leader/DSL or Academy Principal.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will only communicate with students and parents / carers regarding academy matters using official academy systems. Any such communication will be professional in tone and manner.
4. I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions from my own.
5. I will not use communications devices, whether academy provided or personally owned, for bullying or harassment of others in any form.
6. I will not be involved with any online activities, either within or outside academy that may compromise my professional responsibilities or bring the academy, staff, students or community into disrepute.

This includes derogatory/inflammatory comments made on social network sites, forums, blogs and chat rooms.

7. I will ensure that my personal social media profiles have the appropriate privacy settings and include an appropriate disclaimer.
8. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory or those that are inappropriate or that may cause harm or distress to others.
9. I will respect copyright and intellectual property rights.
10. I will not use the academy system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes).
11. I will not install any hardware or software myself. Any new hardware or software installations will only be arranged with the prior permission of the Computing or Online Safety Leader/DSL and Executive Director for ITL and will be installed by the ITL team. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
12. I will ensure that personal data is kept secure at all times and is used appropriately in accordance with Data Protection legislation. Under no circumstances should personal data be stored on any USB memory stick / portable hard drive or any other removable media.
13. I will ensure that images of students and/or adults will be taken, stored and used for professional purposes in line with academy policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the academy network without the prior permission of the parent/carer, or person/s in the image.
14. I will report any known misuses of technology, including the unacceptable behaviours of others.
15. I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
16. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable and may result in disciplinary action.
17. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
18. I have a duty to protect passwords and personal network logins and should log off the network or lock my account when leaving workstations unattended. I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
19. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
20. I understand that network activities and online communications may be monitored, including any personal and private communications made using academy systems.
21. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
22. I will take responsibility for reading and upholding the standards laid out in the AUA. I will support and promote the online safety policy and help students to be safe and responsible in their use of ICT and related technologies.
23. I understand that these rules are designed for the safety of all users and that if they are not followed, academy sanctions will be applied, and disciplinary action taken.

24. I will take due care of any portable ICT equipment given to me to use for academy purposes, and accept that if items (e.g., laptops, tablet computers) are taken offsite, that they are not insured for loss or damage caused by theft or accident. I understand that I will remain solely responsible for their replacement should a theft or accident occur offsite.
25. I understand that portable ICT equipment provided for academy purposes must not be used by non-members of academy staff for any reason.
26. I will undertake Prevent training provided by the academy and understand that I have the duty to report any online activities that could be linked to terrorist activity or radicalisation.

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the academy.

This policy must be signed online via GDPR Sentry.

Appendix C – Student Acceptable Use Agreement

Pendle Education Trust – Student ICT Acceptable Use Agreement (AUA)

The computer systems within the academy are made available to students to further their education. The academy's Acceptable Use Policy has been drawn up to protect all parties who might use the ICT systems. Students who will use the academy's ICT systems should sign this Acceptable Use Statement alongside their parents who share responsibility for ensuring it is adhered to. In the case of students who are too young to sign this agreement (below Key Stage 2), parents are signing on their behalf.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse

For my own personal safety:

- I understand that the academy will monitor my use of the systems, devices, electronic storage and digital communications. This can include when I access academy devices and systems from outside of school and through personal devices.
- I will keep any individual username and passwords safe and secure – I will not share them, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable to a member of staff.
- I will only use academy communication systems (i.e., email, MS Teams, etc) for contacting members of the academy community (staff and students) and will not use my academy email for any other purpose.

Acceptable use of academy devices and facilities

In order to keep the academy ICT equipment and facilities available to everyone, I will:

- Only use academy internet, devices and systems for educational purposes.
- Take responsibility for all actions using my individual accounts, ensuring I do not allow other to have access to them and always log off when I finish using a device.
- Be responsible for my behaviour online and when using academy systems.
- Use the equipment respectfully, responsibly and safely, including not behaving in a way which may cause damage to it.
- Report any damage or faults to a member of staff so that they can be resolved.
- Use email and other online communications as a form of formal written communication, using appropriate language and etiquette.
- Report any inappropriate/offensive materials discovered on the academy ICT system to a member of staff so it can be removed immediately.
- Respect the privacy of other users' files and will not share, alter or delete their work without their permission.
- Develop my research skills and be aware of copyright and intellectual property rights and I will respect this (no illegal downloads or cheating by copying other people's work).

Unacceptable use of academy devices and facilities
In order to keep the academy ICT equipment and facilities available to everyone, I will **NOT**:

- Alter the set up of the equipment, including unplugging cables from computers.
- Access or share any material that is not appropriate or may cause distress or harm to others
- Send any communications which may cause upset or offence to others.
- Take photos or videos of any member of the academy community or use their images from other sources (i.e. academy website). I understand that occasional exceptions may be made where it is required for education purposes and will only do this when directed to and given permission by a member of staff and for that purpose only.
- Waste resources, including printer ink/toner and paper.
- Download any programmes or materials which I am not authorised to by a member of staff and which may cause harm to the academy device or network.
- Bring personal devices into the academy and make use of them on academy systems. This includes portable storage devices such as USB sticks.

Students are advised that their network accounts will be deleted when they leave the Academy and it is the responsibility of the student to save any files before leaving.

Student Declaration: *(for all Key Stage 2, 3 and 4 students (Years 4-11))*
I have read the statement above and agree to the conditions. I understand that the misuse of academy ICT equipment or systems is a serious offence and could lead to sanctions, following the academy behaviour policy, up to and including exclusion.

Name: _____ Form: _____

Signed: _____ Date: _____

Parent Declaration: *(for all students)*
I have read all of the above and agree to ensure my child follows the rules and expectations regarding their use of ICT facilities and systems both in school and at home.

Name: _____

Signed: _____ Date: _____

Appendix D – Visitor Acceptable Use Agreement

Pendle Education Trust – Visitor ICT Acceptable Use Agreement (AUA)

To be read and signed by any adult (including parents) working in the school for a short period of time with access to the school network, including Wi-Fi. The signed copy of this agreement must be kept by the organising member of staff for the event/visit.

This Acceptable Use Agreement is intended to ensure:

- that community users of the Academy and Trust's digital technologies will be responsible users and stay safe while using these systems and devices.
- that Academy/Trust systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices.

I understand that I must use Academy/Trust systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I use on the Academy/Trust site and network:

1. I take responsibility for my use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory or those that are inappropriate or that my cause harm or distress to others.
3. I will respect copyright and intellectual property rights.
4. I will not use any camera or recording equipment (including mobile phones) without the prior agreement of the DSL/Online Safety Leader, Academy Principal or member of SLT. I will ensure that when images of students and/or adults are taken, they are stored and used only for professional purposes in line with academy policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside Pendle Education Trust without the prior permission of the Academy AND the parent/carer (when the subject is a child), or person(s) in the image (when the subject is an adult).
5. I understand that to use Wi-Fi provided by the school, a Trust Certificate must be applied to my device and that network activities and online communications are monitored, including any personal and private communications made using school systems.
6. I will not install any hardware (including removable media, e.g., USB memory sticks and portable hard drives) or software without the prior permission of the Academy Principal, Online Safety Leader or the ITL team. I understand that the use of any removable media may be subject to a checking procedure, which will be carried out by a member of Academy/Trust staff.
7. I understand that these rules are designed for the safety of all users and that if they are not followed, sanctions may be applied (the academy has the right to remove access to school systems / devices and to search personal devices used in the school), disciplinary action taken (if appropriate) and the police and other external agencies informed (if necessary).
8. I understand that the use of personal mobile phones is restricted within the Academies and will comply with the policy within the Academy on their use during the school day.

I have read and understand the above and agree to use the Academy/Trust digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the Academy/Trust) within these guidelines.

Signature _____ Date _____

Full Name _____
(PRINT)

Position/Role/Company _____

Appendix E – Academy-Home Loan Agreement

Pendle Education Trust – ICT Equipment Home Loan Agreement

We are loaning you this computer for the benefit of your child in supporting and developing their education.

This agreement is between the academy and the Named Person who has signed this loan agreement:

1) the Pendle Education Trust Academy (name): ……
2) the Parent/Carer (print name): ……
   of (child's name) …… in (class/form) ……

To be completed by the Academy before the agreement is signed:

Device type: Serial Number:

This agreement governs the use and care of devices assigned to the student. This device can only be used for educational purposes and not for personal use. It can not be loaned to any other person, including family members within the same household.

You will be issued with the device (laptop, tablet, etc) and power supply (charging cable). All issued equipment shall remain the sole property of the academy and is governed by the academy's policies.

This agreement covers the period from the date the device is issued through to the return date of the device to the academy. This may be for the duration of time the child is on roll at the academy, but the academy reserves the right to recall devices at any point. If the child leaves the academy the device must be returned.

If the device is recalled, either to end the agreement or for upgrades and maintenance, it must be returned within 5 days of the request.

The school is not responsible for any costs resulting from the use of the computer and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.

Acceptable Use

The device should be used for its intended purpose of home learning. The terms of the Student Acceptable Use Agreement should be followed and always apply when using the Academy equipment. By signing this, you agree that your child will follow this agreement.

You will be able to install licensed legally purchased software and equipment such as printers and scanners on your computer. You will be able to connect the device to your home internet connection.

All technical support and maintenance must go through the Academy.

Unacceptable Use
The academy monitors the use of this device and students' activity through it and on any academy systems. Safeguarding and security software is installed to monitor and restrict access to inappropriate content online. This should be in addition to your own home security and monitoring of your child's use of the internet.

By signing this, you agree that your child will not carry out any activity that constitutes 'unacceptable use'. This includes, but is not limited to:

- using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- any illegal conduct, or statements which are deemed to be advocating illegal activity
- activity which defames or disparages the Academy or Trust, or risks bringing them into disrepute
- causing intentional damage to ICT facilities or materials
- using inappropriate or offensive language

At no point must the device be taken apart/opened and there must be no changes to the inner hardware.

You must not decorate or change the external face of the device in any way, including affixing stickers.

Reasonable health and safety precautions should be taken when using a computer. The school is not responsible for any damage to person or property resulting from the computer or equipment loaned.

If the student engages in any unacceptable use, the academy will sanction the student in line with the Behaviour Policy. By signing this, you agree to support the academy in this action.'

Data Protection
To keep the data on the device protected, the student must:

- keep the equipment password protected. Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g., asterisk or currency symbol)
- lock the equipment if it is left inactive for a period of time.

By signing this, you agree to ensure your child follows these requirements and will support you child to do so.

There may be occasions when we need you to return the computer to school for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the computer. During this process, technical members of staff may view data or programmes on the computer. The Academy cannot be held responsible for the loss or damage of any data on the computer during this process. You may want to remove data from the computer before its return. It is recommended to make use of the Academy cloud storage (Office 365/Gmail) where this data can be kept online unaffected by any alterations to the device.

Damage/Loss
You have a responsibility to take reasonable care to ensure the security of the computer and connectivity equipment. Reasonable measures should be taken to keep the device safe and to avoid the risk of damage or theft. This includes, but is not limited to:

- storing the device in a secure place when not in use
- not leaving the device on show in a car or at home
- not eating or drinking around the device

- not leaving the device unsupervised in an unsecure area

If the device is damaged, lost or stolen, you must immediately inform the academy. If the device is stolen, you must also immediately report it to the police and get a crime reference number and inform the academy.

If your computer is accidentally damaged, immediately contact the academy. We will do our best to repair the damage, if this is not possible, replacement will be on a case-by-case basis.

You are responsible for the reasonable costs requested by the academy to repair or replace the equipment, and by signing this you agree to honour that.

Consent
I, the parent/carer, have read or had explained and understand the terms and conditions in the home loan agreement. I understand that by breaching the conditions the loan of the device may be withdrawn by the Academy.

Signature _____ Date _____

Appendix F – GDPR Suppliers Assessment for ITL systems

GDPR assessment for new suppliers

For all new suppliers (any company providing a service), the following checks need to be completed before access to our data (data belonging to staff, students, parents, etc.) is set up. As you are the data controllers it is your responsibility to complete these checks to ensure the data you share is as safe as possible.

Name of company/product:	
Website/contact details:	
Request for this to be set up by? (Staff name and academy)	
To be used by which of our academies? (List all)	
What data is going to be shared?	
For what purpose?	
Is there an end date on when we will stop sharing this data?	

Checks to be completed	**Information**
What country or territory is hosting your data? *If the data is hosted within the UK or the EEA it is safeguarded by the GDPR.* *If the data is hosted outside of the UK and EEA it is hosted in a third country. You will need to check on the safeguards that have been put in place to keep the data safe. Are there any standard contractual clauses (SCC's) giving guarantees that the data is as safe as it is in the UK or EEA. If they refer to the EU-US privacy shield (please be aware this was struck down by the European courts as being inadequate) check if they have made you aware that the US government can access your data without consent or your knowledge, therefore not providing the same safeguards as GDPR within the UK or EEA.*	
What system or data center are they using to host your data? *If they are using a well-known hosting site such as Microsoft Azure and Google this should give added protection. If they are using a local server finding out how secure this and the security of the building to give you added peace of mind.*	
Is your data encrypted? *Encrypted data offers another level of protection for your information. Also is the data encrypted in transit and at rest.*	
Does the supplier have any additional security certification schemes and are they part of any SSL features or ISO security standards? *SSL encryption and ISO certification will give you peace of mind that your data is more secure.*	
Can you find access to your rights? *A main part of the GDPR is the rights of the data subject: The right to be informed. The right of access. The right to rectification. The right to erasure. The right to restrict processing. The right to data portability. The right to object. Rights in relation to automated decision making and profiling.*	

How long do they intend to keep your data for? *Check their retention schedules, ensure you are happy with how long they intend to keep your data for.*	
Do they have a data protection officer? *Always good to know who to contact should you have any queries or concerns, and it will also offer additional peace of mind that the supplier takes the protection of data a priority.*	
Do they share the data with a third party? *If they share your data with a third part company, they need to ensure they have checked their privacy policies and given you reassurances about the security and protection of your data.*	

Approved by Executive Director for ITL or ITL Team Leader	
Date this is recorded on GDPR Sentry	