North East Learning Trust

Acceptable Use Policy

Review Date	Reviewer	Approved by	Date Approved	Implementation
	J Barker	Trustees	December 2019	December 2019
September 2021	J Barker	Executive Board	10 July 2021	1 September 2021
September 2023				

Issue No	Date	Description
2	July 2021	Updated 'Links to other policies' to include Online Safety

	Contents	Page No.

1.0 Introduction

The North East Learning Trust promotes the use of technology and understands the positive effects it can have on enhancing the learning and community engagement of students/pupils, we must also ensure that technology is used appropriately. Any misuse of technology will not be taken lightly and will be reported in order for any necessary action to be taken.

This policy is designed to outline responsibilities when using Trust and Academy technology and associated IT systems.

For the purposes of this policy Headteacher may also be read as Executive Headteacher, Headteacher, Head of School.

2.0 Aims of the Policy

- Set guidelines and rules on the use of Trust and Academy IT resources for staff, students/pupils, parents/carers and members, trustees, and governors.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the Trust and Academy policies on data protection, online safety and safeguarding.
- Prevent disruption to the Trust and Academies through the misuse, or attempted misuse, of IT systems.
- Support Academies in teaching staff, students/pupils safe and effective internet and IT use.

3.0 Links with other policies

This policy covers all users of all Trust and Academy IT facilities, including members, trustees, governors, staff, students/pupils, volunteers, contractors, and visitors.

This policy should be read in conjunction with the following Trust and Academy policies:

- Behaviour (students/pupils)
- Code of Conduct for Staff
- Code of Conduct for Members, Trustees and Governors
- Data Protection
- Exclusion
- Online Safety
- Remote Learning Policy
- Safeguarding
- Disciplinary (staff)

Breaches of this policy will be dealt with in accordance with the relevant Trust and Academy policies and procedures.

4.0 Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools

This policy complies with the Trust's Articles of Association and Funding Agreement.

5.0 Privacy

The Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity, and accuracy. This applies to all data the Trust and its Academies store on its network regarding staff, students/pupils, and other appropriate persons it deals with whilst carrying out its functions.

The Trust will only process data in line with its lawful basis to uphold the rights of both students/pupils and staff and other third parties.

In order to protect the safety and wellbeing of students/pupils, and to protect the Trust from any third party claims or legal action against it, the Trust and the Academy may view any data, information or material on the Trust's IT systems (whether contained in an email, local or remote networks, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The Trust's Data Protection Policy details the lawful basis under which the Trust is lawfully allowed to do so.

The Trust disclaimer that automatically appears at the end of each of your emails notifies the recipient that any email correspondence between you may be monitored. You must not

remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an email that the Trust may monitor the content of their email.

For further information or to clarify any of the points raised in this policy please contact the Trust's Data Protection Officer.

6.0. Unacceptable use

The following is considered unacceptable use of the Trust and Academy IT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the Trust and/or Academy IT facilities includes:

- Using the Trust and/or Academy IT facilities to breach intellectual property rights or copyright.
- Using the Trust and/or Academy IT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the Trust and/or Academy policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate.
- Activity which defames or disparages the Trust and/or its Academies, or risks bringing the Trust and/or its Academies into disrepute.
- Sharing confidential information about the Trust and/or its Academies, its students/pupils, or other members of the school community.
- Connecting any device to the Trust and/or Academy IT network without approval from authorised personnel.
- Using local or remote storage mediums (including cloud storage) to copy or move data from the network without prior approval.
- Setting up any software, applications, or web services both locally or externally without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the IT facilities, accounts, or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities.
- Causing intentional damage to IT facilities.
- Removing, deleting, or disposing of IT equipment, systems, programs, or information without permission by authorised personnel.
- Accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the Trust and/or its Academies.
- Using websites or mechanisms to bypass the Trust and/or its Academies filtering or monitoring systems.

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust and/or Academy IT facilities.

7.0 Exceptions from unacceptable use

Where the use of Trust and Academy IT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the discretion of the Headteacher.

Requests must be submitted in writing to the Headteacher who will discuss the request with the Director of IT. The member of staff will be informed, in writing, of the decision. The Headteacher's decision is final.

8.0 Sanctions

Students/Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the relevant Trust and Academy policies.

9.0 Staff access to Trust and Academy IT facilities and materials

9.1 Access rights

The Director of IT manages access to the Trust and Academy IT facilities and materials for all staff.

That includes, but is not limited to:

- Computers, tablets, and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Trust and Academy IT facilities. This must be kept safe and never shared, in the event of an incident the user account identified by the logs or audit report could be held accountable for any unacceptable use as defined in this policy.

All users of the Trust and/or Academy IT facilities will have clearly defined access rights to Trust and/or Academy systems, files, and devices.

Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert Director of IT immediately.

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

All access is logged by username, in the event of an incident the holder of the account may be held accountable for any misuse.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Director of IT and/or Data Protection Officer immediately.

Staff requesting modifications to file sharing location must follow the following process:

- Request for modification from individual staff member and is submitted by logging into the helpdesk ticket system
- Change is validated by SLT/Data manager
- Change is actioned by helpdesk staff
- Change is validated by helpdesk manager
- Request is closed and communicated to requester

9.2 Use of email

Each member of staff is issued with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the Trust has provided.

Staff must not share their personal email addresses with parents/carers and students/pupils and must not send any work-related materials using their personal email account.

Staff must use the BCC facility when sending group emails to parents/carers.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Staff must not communicate in inappropriate way with colleagues through emails, and care should be taken to ensure that emails are not rude and/or aggressive in both content and tone and must not in any circumstances contain ‘email shouting’.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user’s inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email, this should include a consideration as to whether email is the correct medium on a case by case basis. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. It is also possible to block the forwarding of such data once received, if there is any uncertainty as to whether a mail should be sent and to what degree protected then clarification must be sort from the DPO.

If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Data Protection Officer immediately and follow The Trust's data breach procedure.

Staff must not give their personal phone numbers to parents/carers and/or students/pupils. Staff must use phones provided by the Trust and/or Academy to conduct all work-related business.

Trust and Academy phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT unacceptable use as set out in section 6.

9.3 Personal use of IT

Staff are permitted to occasionally use Trust and/or Academy IT facilities for personal use subject to certain conditions set out below. Personal use of IT facilities must not be overused or abused. The Trust may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during working hours.
- Does not constitute 'unacceptable use', as defined in section 6.
- Does not takes place when students are present.
- Does not interfere with their jobs or prevent other staff or students/pupils from using the facilities for work or educational purposes.

Staff may not use the Trust and/or Academy IT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the Trust and/or Academy IT facilities for personal use may put personal communications within the scope of the Trust's IT monitoring activities (see section 9.7). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Trust's Staff Code of Conduct.

Staff should be aware that personal use of IT (even when not using Trust and/or Academy IT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students/pupils and parents/carers could see them.

Staff should take care to follow the Trust's guidelines on social media (Appendix 1) and use of email (section 9.2) to protect themselves online and avoid compromising their professional integrity.

9.4 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The Trust has guidelines for staff on appropriate security settings for social media accounts (Appendix 1).

9.5 Remote access

Staff accessing the Trust and Academy IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the Trust and Academy IT facilities outside the school and take such precautions as the Director of IT may require from time to time against importing viruses or compromising system security.

The use of public access points should be avoided unless their integrity can be verified, open 'hot spots' operated by coffee shops, for example can be hijacked which may expose your data to abuse/breach.

One form of protection against unverified public access points is a system called Virtual Private Network (VPN), VPN's create a secure tunnel through unprotected networks making it far less likely for data to be intercepted whilst in transit. You should consult IT services before using any VPN, these systems can trigger alerts or block access to Office365 services.

The use of IP masquerading or access anonymisers must be avoided as such systems are often used to avoid the monitoring of internet traffic (for the purposes of profiling or advertisements). These systems, like VPN's may cause access attempts to be blocked or flagged as the mechanism may also be used by an attacker.

The IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

The Data Protection policy can be found on the following websites:

www.nelt.co.uk
www.ashingtonacademy.co.uk
www.bedlingtonacademy.co.uk
www.browneyacademy.co.uk
www.diamondhalljunioracademy.co.uk
www.easingtonacademy.co.uk
www.hermitageacademy.co.uk
www.ryehillsacademy.co.uk
www.sacristonacademy.co.uk
www.teesdaleschool.co.uk
www.theacademyatshottonhall.co.uk

9.6 Trust and Academy social media accounts

The Trust and all its' Academies have an official Facebook and Twitter page, managed by the Communications and Marketing Team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The Trust has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

We ask all members of staff, members, trustees, governors, visitors, and contractors to sign the agreement in appendix 2

10.0. Students/Pupils access to Trust and Academy IT facilities

10.1 Accessibility

The following IT facilities are available to students/pupils:

- Computers and equipment in the Academy's IT suite are available to students/pupils only under the supervision of staff.
- Specialist IT equipment, such as that used for music or design and technology must only be used under the supervision of staff.
- Students/Pupils will be provided with an account linked to the Academy's virtual learning environment, which they can access from any device by using the appropriate URL.
- Sixth-form students can use the computers independently for educational purposes only.

10.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the Academy has the right to search students/pupils phones, computers or other devices for pornographic images or any other data or items banned under Academy rules or legislation.

The Trust can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the Academy rules.

10.3 Unacceptable use of IT and the internet

The Academy will sanction students/pupils, in line with the Academy's Behaviour Policy, if a student/pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using IT or the internet to breach intellectual property rights or copyright
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust and/or Academy policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate
- Activity which defames or disparages the Trust and or the Academy, or risks bringing the them into disrepute
- Sharing personal credential information such as passwords
- Sharing confidential information about the Trust and/or its Academies, other students/pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust and/or Academy IT facilities

- Causing intentional damage to IT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

We ask students/pupils to sign the agreement in appendix 2.

11.0 Parents/Carers access to IT facilities and materials

11.1 Accessibility

Parents/carers do not have access to the Trust and/or Academy IT facilities as a matter of course.

However, parents/carers working for, or with, the Academy in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the Trust and/or Academy IT facilities at the discretion of the Headteacher.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

11.2 Communicating with or about the Trust and its Academies online

We believe it is important to model for students/pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the Academy through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 2.

12.0 Visitor access to Trust and Academy IT facilities and materials

Visitors to the Trust premises and/or Academies will be permitted to use the Academy's Guest Wi-Fi.

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action. Should staff wish to sponsor their guest for Wi-Fi access then the appropriate procedure must be followed, this involves the sponsor making the guest aware of their responsibilities as well as creating an access account.

13.0 Monitoring of network and use of IT facilities

The Trust reserves the right to monitor the use of its IT facilities and networks. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs/device history/IP addresses/interactions
- Any other electronic communications

Only authorised IT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The Trust monitors IT use in order to:

- Obtain information related to Trust and/or Academy business
- Investigate compliance with Trust and/or Academy policies, procedures, and standards
- Ensure effective school and IT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

14.0 Data protection

All personal data must be processed and stored in line with the Data Protection Act 2018 and the Trust's Data Protection policy.

The policy is published on the Trust and all Academy websites.

15.0 Data security

The Trust takes steps to protect the security of its computing resources, data, and user accounts. However, security cannot be guaranteed. Staff, students/pupils, parents/carers, and others who use the Trust's IT facilities should use safe computing practices at all times.

The use of removable media or other storage mediums to transfer data should be considered as a last resort in all instances when transferring data outside of Trust systems.

15.1 Passwords

All users of the Trust and Academy IT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. Care must be taken not to store passwords in a way that is accessible to others, the use of notebooks or notes to record such information is unacceptable.

Members of staff or students/pupils who disclose account or password information may face disciplinary action. Parents/carers or volunteers who disclose account or password information may have their access rights revoked.

15.2 Encryption

The Trust ensures that its devices and systems have an appropriate level of encryption.

Staff may only use personal devices (such as computers, tablets, and phones) to access school data and work remotely. Personal data (such as student/pupil information) should not be copied and/or stored on personal devices. For the benefit of clarity this refers to the use of personal devices to access data stored within the Trust secure network, such access is low risk as the data remains on the secure network (if data is transferred outside of the secure network it becomes uncontrolled and at risk).

In exceptional circumstances, the Headteacher may authorise a member of staff to use a personal device to store personal data, however this will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Director of IT.

15.3 Software updates, firewalls, and anti-virus software

All of the Trust and/or Academy IT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the Trust and/or Academy IT facilities. If it is suspected that these safeguards are not working correctly then it is the user's responsibility to inform the IT service.

Any personal devices using the Trust and/or Academy network must all be configured in a way that does not compromise the network or other users. It is expected that all devices will be free from malware and also up to date with relevant security updates, if there is any doubt then IT must be consulted before any connection is made.

15.4 Internet access

All wireless internet connections used across the Trust are secure.

16. Monitoring

The implantation of this policy is monitored by the Headteacher and staff and students should report any issues to the Network Manager in school.

Appendix 1

Personal Social Media Guidelines for Staff, Members, Trustees and Governors

This policy applies to all personal webspace such as social networking sites (for example *Facebook*, *Twitter*), blogs, microblogs, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *Flickr* and *YouTube*.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

The following principles must be observed by all staff:

- You must not represent your personal views as those of the Trust and/or any of its Academies on personal social media.
- You must not communicate with students who are currently enrolled at the Academy (or those who have recently left and who are under the age of 18) on personal social media with the exception of a genuine emergency situation, in which case you should notify a senior member of staff of the communication as soon as possible.
- Staff members must not have any contact with students/pupils' family members through personal social media – any attempts by family members and/or friends to communicate with staff should be directed towards formal school communication channels such email, telephone, or face-to-face meetings.
- You must not discuss personal information about students/pupils, staff, and other professionals you interact with as part of your job on personal social media.

- You must not use personal social media to attack, insult, abuse or defame students/pupils, their family members, colleagues, other professionals, or other organisations.
- You must decline 'friend requests' or 'follows' from students/pupils you receive in your personal, private social media accounts. Instead, discuss these in general terms in class and signpost students/pupils to follow official Trust and Academy accounts.
- Information staff members have access to as part of their employment, including personal information about students/pupils and their family members, colleagues or corporate information must not be discussed on personal social media.
- Photographs, videos, or any other types of image of students/pupils and their families must not be published on personal social media.
- School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.
- The Trust and/or any Academy logos must not be used or published on personal social media.
- Staff should never provide references for other individuals on social or professional networking sites either positive or negative. These can be attributed to the organisation and create legal liability for both the author of the reference and the Trust.

Social media should never be used in a way that breaches any policy of the Trust and any of its Academies. If an internet or social media post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

(a) breach our obligations with respect to the rules of relevant regulatory bodies.
(b) breach any obligations contained in those policies relating to confidentiality.
(c) breach our disciplinary policy or procedures.
(d) harass or bully other staff, students/pupils, parents/carers or third parties in any way.
(e) unlawfully discriminate against other staff, students/pupils, parents/carers or third parties.
(f) breach our data protection policy (for example, never disclose personal information about a colleague online).
(g) breach any other laws or regulatory requirements.

Staff who breach this policy, or any of the above policies may be subject to disciplinary action up to and including termination of employment.
On leaving service, staff members must not contact students/pupils by means of personal social media sites. Similarly, staff members must not contact students/pupils from their former schools' by means of personal social media.

Privacy
Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy.
Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.
It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Legal Framework
All employees of the Trust are bound by their contractual terms and conditions of employment and various legislation which protects the confidential information they have access to during the course of their work. Disclosure of confidential information on social media may be in breach of a number of laws and professional codes of conduct, including:

- The Human Rights Act 1998
- Common law duty of confidentiality
- The Data Protection Act 2018

Confidential information includes, but is not limited to:

- All confidential information (however recorded or preserved) which would be regarded as confidential by a reasonable person including but not limited to the business affairs, operations, processes, know-how, clients, students/pupils, suppliers, business plans or intentions, or market opportunities of the Trust and/or its Academies.
- Any information covered by the Data Protection Act 2018, including but not limited to student/pupil and employee records.
- Information divulged in the expectation of confidentiality.
- Trust, Academy and/or corporate records containing organisationally or publicly sensitive information.
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and politically sensitive information.
- Staff members should also be aware that other laws relating to libel, defamation, harassment, and copyright may apply to information posted on social media, including the following legislation (as amended and re-enacted from time to time):
    - Defamation Acts 2013
    - Data Protection Act 2018
    - Protection from Harassment Act 1997
    - Criminal Justice and Public Order Act 1994
    - Malicious Communications Act 1998
    - Communications Act 2003
    - Computer Misuse Act 1990, and
    - Copyright, Designs and Patents Act 1988.

The Trust could be held vicariously responsible for acts of our employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyber-bullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render the Trust liable to the injured party.

Monitoring and Removal of Content

The Trust reserves the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems.

The Trust reserves the right to request the removal of any Trust and/or Academy related content from any staff personal social media sites. A failure to comply with such a request may in itself result in disciplinary action.

Appendix 2

Technology acceptable use agreement

This acceptable use agreement is designed to outline responsibilities when using technology, whether this is via personal devices or Trust and/or Academy devices or on/off all Trust and Academy premises and applies to all staff, members, trustees, governors, volunteers, contractors and visitors.

Please read this document carefully and sign below to show that you understand and agree to the terms outlined.

Using technology in school

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the Headteacher.
- I will only use the approved email accounts that have been provided to me.
- I will ensure a professional etiquette is maintained at all times when using Trust systems.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any students/pupils, staff or third parties unless explicit consent has been received.
- I will not use unsanctioned external systems, services, or storage without approval.
- I will ensure that any personal data is stored in line with the Data Protection Act 2018.
- I will delete any chain letters, spam, and other emails from unknown sources without opening them. Persistent unsolicited or suspicious email should be reported to the IT service.
- I will ensure that I obtain permission prior to sharing and/or accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share Trust and/or Academy related information with students/pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto Trust and/or ICT systems unless authorised to do so by the Director of IT and/or Headteacher.
- I will ensure any Trust and/or Academy owned device is working well, with no errors or warnings that may indicate it is at risk from any threats and that I will check this on a constant basis.

- I will only use recommended removable media and will keep this securely stored in line with the Data Protection Act 2018.
- I will only store data on removable media or other technological devices that has been encrypted of pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary, and which is encrypted.
- I will provide removable media to the IT service for safe disposal once I am finished with it.

Mobile devices

- I will only use Trust and/or Academy owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.
- I will not use mobile devices to take images or videos of students/pupils or staff unless consent has been sought from the individual(s) in the images or videos.
- I will not use mobile devices to send inappropriate messages, images, or recordings.
- I will ensure that personal and Trust and/or Academy owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the Wi-Fi system using personal mobile devices if I am aware that the device may not be up to date with security software and updates.
- I will not use personal and Trust and/or Academy owned mobile devices to communicate with students/pupils or parents/carers.
- I will not store any images or videos of students/pupils, staff, or parents/carers on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of students/pupils, staff, or parents/carers for the activities for which consent has been sought.
- I will ensure that any school data is only stored on personal mobile devices if it is encrypted by the IT service or pseudonymised and give permission for the IT service to erase and wipe data from my device if it is lost or as part of exit procedures.

Social media and online professionalism

- If I am representing the Trust and/or one of its Academies online, e.g. through blogging or on Trust and/or Academy social media accounts, I will express neutral opinions and will not disclose any confidential information regarding the Trust and/or its Academies, or any information that may affect its reputability.
- I will not use any Trust and/or Academy owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Headteacher before accessing the site.
- I will not communicate with students/pupils or parents/carers over personal social networking sites.
- I will not accept 'friend requests' from any students/pupils or parents/carers over personal social networking sites.

- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the Trust and/or its Academies on any social networking sites which may affect the reputation of the Trust and/or its Academies.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students/pupils, staff, or parents/carers, on any online website.
- I will not post or upload any images and videos of students/pupils, staff, or parents/carers on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of students/pupils, staff, or parents/carers for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to students/pupils or parents/carers – any contact with parents/carers will be done through authorised contact channels.

Working at home

- I will adhere to the principles of the GDPR when taking work home.
- I will ensure I obtain permission from the Headteacher and DPO before any personal data is transferred from a Trust and/or Academy owned device to a personal device.
- I will ensure that before any data is transferred from a Trust and/or Academy owned device to a personal device is encrypted or pseudonymised as is verified by the IT service or DPO.
- I will ensure my personal device has been assessed for security by the IT service before it is used for lone working.
- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone working.
- I will always log out of systems and lock my equipment at home when they are not in use and/or unattended to avoid any unauthorised access
- I will act in accordance with the Trust's E-Safety Policy when transporting Trust and/or Academy equipment and data.

Training

- I will ensure I participate in any e-safety or online training offered to me and will remain up to date with current developments in social media and the internet as a whole.
- I will seek assistance if I am unsure about any aspect of e-safety or have questions around best practise and/or gaps in my knowledge.
- I will ensure that I allow the Director of IT and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for students/pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to students/pupils as required.

Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Acceptable Use Policy.

- I will ensure that I report any misuse by students/pupils, or by staff members breaching the procedures outlined in this agreement, to the Headteacher.
- I understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the Headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedure if I breach this agreement.
- I understand that I am responsible for reporting suspected actual account or data breaches, if I have any concerns, I will consult Headteacher and/or Director of IT immediately.

Acceptable use of the Trust and/or Academy IT facilities and the internet: agreement for staff, governors, volunteers and visitors (This form will be securely disposed of when you are no longer employed/involved in the Trust and/or Academy)

Name:
Academy:
Position:

When using the Trust and/or Academy IT facilities and accessing the internet in any Trust or Academy premises, or outside the Academy on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the Trust and/or Academy reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the Trust and/or Academy network
- Share my password with others or log in to the Trust and/or Academy network using someone else's details
- Share confidential information about the Trust and/or Academy, its students/pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the Trust and/or Academy

I understand that the Trust will monitor the websites I visit and my use of the Trust and/or Academy IT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the Trust's data protection policy.

I will let the designated safeguarding lead (DSL) and IT manager know if a student/pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the Trust and/or Academy IT systems and internet responsibly and ensure that students/pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Acceptable use of the internet: agreement for parents and carers (When your child leaves the Academy this form will be disposed of securely)

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our Academy.

The Academy uses the following channels:

- Official Facebook page
- Email/text groups for parents/carers (for school announcements and information)
- Our virtual learning platform

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the Academy via official communication channels, or using private/independent channels to talk about the Academy, I will:

- Be respectful towards members of staff, and the Academy, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the Academy's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the school cannot improve or address issues if they are not raised in an appropriate way
- Use private groups, the Academy's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other students/pupils. I will contact the Academy and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

• I will not covertly or otherwise use a device to record any event and/or meeting in school without the prior consent of all parties present.	
Signed:	**Date:**

Acceptable use of the Trust and Academy IT facilities and internet: agreement for students (This form will be securely disposed of when you leave the Academy)

Name of Student:

When using the Trust and/or Academy IT facilities and accessing the internet in the Academy I will not:

- Use them for a non-educational purpose
- Use them without a member of staff being present, or without permission from a member of staff
- Use them to break Academy rules
- Access any inappropriate websites
- Access social networking sites (unless a member of staff has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Covertly or otherwise record staff and/or students on any device without their prior consent.

I understand that the Trust and Academy will monitor the websites I visit and my use of the Trust and Academy IT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the Trust and Academy IT systems and internet responsibly.

I understand that the Academy can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (student):	**Date:**

Parent/carer agreement: I agree that my child can use the Trust and Academy IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the Trust and Academy IT systems and internet, and for using personal electronic devices in the Academy, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Acceptable use of the school's IT facilities and internet: agreement for pupils (This form will be securely disposed of when you leave the Academy)	
Name of pupil:	**Date of birth:**
When I use the school's IT facilities (like computers and equipment) and get on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break school rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms • Open any attachments in emails, or click any links in emails, without checking with a teacher first • Use mean or rude language when talking to other people online or in emails • Share my password with others or log in using someone else's name or password • Bully other people I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the Trust and Academy IT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the Trust and Academy IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the Trust and Academy IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**