Ascend Learning Trust

Acceptable Use Policy

Policy Owner:	Trust IT Lead
Date of issue:	September 2024
Policy Level:	Tier 1
Approved by:	Full trust board
Next Review:	September 2025

Contents

Version Control

Version	Details	Author	Date
1.0	Policy formation	Jeremy Masson	1st September 2024
2.0			

Related Policies

- Ascend Cyber Security Policy
- Ascend Data Protection Policy
- Ascend Online Safety Policy
- Ascend AI Policy
- Ascend Email Policy

Introduction

This policy applies to Ascend Learning Trust as a whole which includes all the schools within the trust.

In implementing the policy and associated procedures individual headteachers and trust staff must take account of any advice given to them by the ALT Trust IT Lead, the ALT CEO and/or Board of Trustees.

This policy is subject to the scheme of delegation approved for Ascend Learning Trust. If there is any ambiguity or conflict then the scheme of delegation and any specific scheme or alteration or restriction to the scheme approved by the Board of Trustees, takes precedence.

If there is any question or doubt about the interpretation or implementation of this Policy, the Ascend Trust IT Lead should be consulted.

Policy Statement

Information and communications technology (ICT) is an integral part of the way Ascend Learning Trust works, and is a critical resource for pupils, staff, trustees, governors, volunteers, and visitors. It supports teaching and learning, and the pastoral and administrative functions of the whole trust.

However, use of ICT resources and facilities within the Trust could also pose risks to data protection, online safety, and safeguarding. All users who access IT systems operated by the trust should be entitled to safe access at all times. This policy is intended to provide a working framework for staff to uphold the positive use of technology whilst providing a safe learning environment and protecting data that is managed by the trust.

This policy aims to:

- Set guidelines and rules on the use of trust ICT resources for staff, pupils, parents, trustees and governors.
- Establish clear expectations for the way all members of the trust community engage with each other online.
- Support the trust's policies on data protection, online safety, and safeguarding.
- Prevent disruption that could occur to the Trust through the misuse, or attempted misuse, of ICT systems.
- Support the Trust in teaching pupils safe and effective internet and ICT use.

This policy covers all users of the trust's ICT facilities, including trustees, governors, staff, pupils, volunteers, contractors, and visitors.

The acceptable user policy agreement is in place to prevent hard to the trust's online systems and computer hardware, and day to day running of both individual schools and the trust as a whole. **This policy sets out the trust's expectation of everyone using its equipment and/or internet access. Illegal or immoral use is not acceptable and will result in relevant disciplinary action.**

Relevant Legislation and Guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- 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
- Education and Inspections Act 2006
- Keeping Children Safe in Education
- Searching, screening and confiscation: advice for Trusts
- National Cyber Security Centre (NCSC): Cyber Security for Trusts
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

- Meeting digital and technology standards in Trusts and colleges
- DfE BYOD Guidance
- NCSC BYOD Guidance

Provision of School Information and Communication Tools

The trust will provide information and communications technology to be used in connection with the operation of each individual school and the trust as a whole. This may include but is not limited to computers/laptops, landline phones, VoIP phones, mobile/smart phones, printers, photocopiers, and any other means of storing, copying, and transmitting data. As such, these tools are principally intended to be used for trust and/or school purposes. Inappropriate use of trust communication tools may give rise to disciplinary action. The Trust reserves the right (for trust and/or school purposes or as may be required by law) to review the use of, and to inspect all material created by or stored on, these communication tools (See also the section on "Privacy" below). At no point should any Trust device be used to access personal social media accounts.

The trust provides Wi-Fi connectivity for staff, students and some authorised visitors; where appropriate, this allows all internet activity to be accountable to the individual on any device by means of logging in on a daily basis. This is implemented through a voucher or credential based system to prevent misuse of systems, and ensure the correct device is logged against that individual.

Use of trust-provided communication equipment constitutes acceptance of the trust's right to monitor communications and access files that are made on or with that equipment.

Trust Property

Trust-provided communication equipment, as well as all data, files and messages produced, transmitted, or stored using such equipment, are and remain the property of the trust, and are subject to reasonable inspection, on request.

Trust equipment may be issued to a range of stakeholders including employees, volunteers, trustees or governors and pupils. Equipment may be loaned or used by stakeholders on a short term basis (ie for a couple of hours) or on a long term basis (ie for the duration of their employment). At all times, trust equipment should be treated respectfully and care should be taken to ensure that equipment does not become damaged during the period of use. This extends to the correct storage and carrying of equipment (for example, using the provided laptop case). If equipment is lost, stolen or damaged due to negligence or abuse, the trust reserves the right to seek to recover necessary costs up to the cost price of replacement equipment. In such circumstances, the amount and terms of recovering said costs will be determined at the time of the loss and in discussion with relevant parties.

Where trust equipment will be used outside of an individual trust building, and in particular at the home of an employee, volunteer or student, the responsibilities for safe care and storage of the equipment remain with the individual to whom the equipment has been provided. The trust recommends that where equipment is used outside of a trust building that the individual loaning the equipment has suitable insurance cover in place and/or has ensured that the device will be covered under a household insurance policy.

Trust equipment should be returned upon a reasonable request from the trust or when the individual to whom the property has been loaned ceases to be involved with the trust. Failure to return all equipment, or if it is returned in a damaged condition, the trust reserves the right to seek to recover the costs, as outlined above. The specific caveats below apply:

Employees

All employees must return all trust provided communication tools upon termination of their employment that are in their possession (laptop computers, mobile phones, etc). Additionally, they should ensure that all electronic data produced and stored on them is also returned alongside and any duplicates of such data (such as stored on a hard drive) should be returned to destroyed. The trust reserves the right to deduct any costs to replace, repair or recover communication tools from an employee's final salary payment.

Students

Any student in possession of a trust device (such as a tablet or laptop) is reminded that the item remains the property of the trust and should be returned when you cease be a pupil registered at the school. The trust will seek to recover the costs of items that are not returned, or are returned damaged, by invoicing the legal parent/guardian.

Passwords

The trust expects each individual user to be responsible for their personal password security and will consider them responsible for actions taken when their passwords are used. Individual users are reminded that they should not reveal their passwords to anybody.

Never leave a computer logged on and unattended. When leaving a computer or laptop, the trust expects all users to lock the screen. Users are also reminded of the importance of logging off from shared devices; this not only protects the integrity of the data, but also ensures ICT resources operate in a more efficient manner.

All users of trust systems must set and maintain the security and confidentiality of their own password. If at any time an individual user believes their password to be compromised, they must report it to an appropriate individual **immediately.**

Employees: report to your line manage and the trust IT support Team

Students: report to an appropriate member of school staff such as a tutor, a teacher of the reception team, who will support in notifying the relevant IT support team.

Passwords must be set following the NCSC guidance on secure password setting, available here: NCSC.GOV.UK

Passwords **must** be changed at least once every 180 days (at least once per academic year), be a minimum of 8 characters, and employ the three random word guidance set by the NCSC.

Passwords must also have a mixture of uppercase, lowercase, numbers and special characters in order to meet complexity requirements. It is best to use passwords that are not easy to guess, such as your own name or date of birth. An example of a strong password is: CatWoodBasket2!

Users will also be invited to sign up for 2FA (two factor authentication) for external access to email, using secondary information to secure their account.

Software

It is the trust's express policy to pay for the software it uses. No user must load, use, store or transmit any unlicensed or unauthorised software or applications on any trust-provided computer or mobile/smart phone, whether situated on trust premises or off-site, under any circumstances.

Any specific requests for additional licenses or software programs must be discussed with IT support.

Virus Protection

Virus protection software is installed on all trust computers which is automatically updated. All users are responsible for ensuring it is allowed to regularly update. Individual users must never take any action that would circumvent virus protection. Additional precaution is advised around email attachments and executable programs imported from the Internet, which may contain viruses, Trojans, worms and so on.

Simple steps can be taken when looking at e-mail: Do you recognise the sender? Hovering over a link, does the address look genuine? Were you expecting this e-mail? Please see the Ascend Email Policy for further guidance. If any items look suspicious, please check with IT support before proceeding.

Our anti-virus products will block the ability to download known viruses or malware and scans are routinely run across all devices. However, all users are reminded of being vigilant whenever using Trust IT.

If you believe that your computer has a virus, or you have opened an email that contains malicious software and may therefore have exposed the trust systems, you must notify the IT Support team as a matter of urgency. IT Support will then guide you on the necessary actions to take depending on the circumstances and situation.

Use of Trust-Provided Equipment by Third Parties

Trust provided equipment must principally be used by the person to whom it has been provided. At no point should friends, relatives or other third parties who are not employed by or students of the trust and its schools be allowed to use any Trust-provided equipment. Individual users should never knowingly allow another trust based user the use of assigned equipment for inappropriate purposes.

Non-Trust personnel who may require access to Trust-provided communication tools for legitimate purposes (e.g. clients or contractors) must first be provided with a copy of this policy and sign a written agreement confirming that they will comply with its provisions.

BYOD / Use of Personal Devices

The Trust allows the use of personal devices where appropriate. Measures have been taken appropriately to comply with both DfE BYOD Guidance and NCSC BYOD Guidance.

The use of WIFI for user personal devices will require individuals to authenticate on a daily basis as and when they may require access to the Trust network, this authentication allows the device to be traceable to the individual login, as per Trust user access, and as suggested by DfE and NCSC.

Under no circumstances should a personal device be used for taking or storing photographs/videos of students.

The Trust operates a modern Wi-Fi system, compatible with the latest security standards, it should be noted however that this can mean that some devices may be unsupported.

Remote Access

We allow key stakeholders, where possible, to access the Trust's ICT facilities and materials remotely. Remote access connections are specific to each individual school and users should follow their local method.

For Trust owned devices, BitLocker encryption will be implemented; this should not be stored with the laptop, and only used for accessing the device.

In order to minimise attempts to compromise Trust systems, secure VPN access is restricted to the United Kingdom only, as recommend by the NCSC and DfE.

When accessing the Trust's ICT facilities and materials remotely, users must abide by the same rules as those accessing the facilities and materials on site. All users must be particularly vigilant if they use the Trust's ICT facilities outside the Trust on a personal device and take suitable precautions such as having appropriate and up to date anti-virus software.

Our ICT 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 the Trust's data protection policy.

Please see Trust Data Protection Policy for further guidance.

Privacy

The Trust will not frivolously or maliciously invade an individual user's privacy. However, because Trust-provided communication tools are principally intended for business and/or school purposes, individual rights to privacy in this context are limited, and users should not expect information created, transmitted or stored on Trust communication systems to remain private.

In addition to routine access for maintenance and upgrades, the Trust is entitled to review electronic messages, files, and data without prior notice, in various circumstances, including (but not limited to):

- Investigating alleged misconduct or behaviour
- Investigating complaints that Trust resources are being used to transmit discriminatory or offensive messages or otherwise infringe upon or violate any other person's rights
- Discovering the presence of illegal material or unlicensed software
- Counteracting theft or espionage
- Responding to legal proceedings that call for the disclosure of electronically stored evidence
- Investigating indications of impropriety.

Under the GDPR and FOI legislation, the trust may need to access personal data contained within email and/or on trust devices issued to staff, students and other stakeholders, where a Subject Access Request has been received.

File Storage and Archiving

Users are encouraged to create folders in order to keep files and email records tidy, to ensure efficient working, and to facilitate retrieval of information where relevant. Individual users should review the files they store on Trust systems for relevance on a regular basis, and transfer anything that is no longer current to an archive folder. Remember that files containing work-related information are the property of the Trust and should be retained for future reference in the same way that paper files would be.

Even though users may delete messages from their own user areas, they may remain on recipients' computers or on the Internet indefinitely; therefore, users should never exchange or upload any content or opinions which they may later regret.

The Internet

The Trust provides Internet access for legitimate use. Often, it is the most efficient means of finding out information or communicating with others. However, this is not always the case, users are encouraged to consider whether there may be quicker and more effective ways to achieve their objectives.

Users are reminded to be aware of copyright issues when downloading or copying data from the Internet. Just because it is easy to copy material electronically, that does not mean it is legal to do so. Most information available on the internet is protected by copyright in the same way as physical materials like books, CDs or

DVDs. Breaching copyright using Trust equipment could result in the Trust having to pay substantial damages to the copyright owners, and may result in action being taken under an appropriate policy such as disciplinary or behaviour policy. It is therefore important that users familiarise themselves with the copyright conditions of the information they are looking at before it is downloaded or copied.

Some websites may contain inappropriate or offensive images or data, and the Trust reserves the right to log, monitor or block incoming and outgoing Internet traffic from those sites. If you inadvertently connect to sites that contain sexually explicit, racist, violent or other potentially offensive material, you must immediately disconnect and advise your manager, Teacher or IT Support that these sites are accessible, so that blocking action may be taken. The ability to connect to them does not imply that the Trust condones the visiting of such sites.

In order to comply with the filtering and monitoring responsibilities outlined in statutory safeguarding legislation, the trust has processes in place to monitor the use of the internet and devices. These processes are regularly tested and if any user attempts to access websites which may contain inappropriate content and/or conduct searches which may cause concern for the safety and/or welfare of that individual user, the trusts safeguarding processes will apply and key personnel will follow up with individual users.

Users must not under any circumstances use Trust equipment to access any inappropriate sites; contravention of this rule will result in disciplinary action.

Email

Email is a tool provided by the Trust to facilitate the effective communication between different users and to ensure efficient operation of the work of the trust. Individual email accounts must only be used for messages and attachments relating to the work of the Trust. The Trust reserves the right to inspect the contents of any emails sent or received by any user.

Email conduct must remain professional and polite at all times; individual users must never send out any email or attachment that might show the Trust in an unprofessional light. Email must never be used to express racist, sexist, or otherwise offensive opinions, either inside or outside the Trust. Inappropriate use of email will be investigated under an appropriate policy depending on the user, such as disciplinary for employees, or the behaviour policy for students.

Please be security conscious. Email is **not** private; messages can be intercepted or wrongly addressed and are easily forwarded to third parties. Users must not allow anyone else to use their email ID and password, or leave their email logged on and unattended so that others could interfere with it**. Individual users will be held responsible for any inappropriate email activity using their accounts.** Similarly, individual users must not send out emails purporting to be somebody else, and must not read other people's emails without their express permission. Caution is also advised when providing a trust email address to third parties such as signing up to trials, mailing lists. This helps to minimise the receipt of junk mail.

The Data Protection Act 2018 covers information stored on email as well as other media, so care must be taken if emails contain any “personal data”, i.e. any information about a living identifiable individual, such as their name, home address, home phone number, personal email address etc. An obvious example would be the receipt, storage or transmission of candidates’ CVs. Such data must not be collected without the person’s knowledge, it must not be disclosed or amended except for the purpose for which it was collected, and it must be accurate and up to date. Particular care must be taken if the data is confidential or sensitive (e.g. contains information about medical conditions, political or religious beliefs etc.). The individual in question has the right to inspect what is held about him or her on the email system, to demand correction of inaccurate information, to request blocking or erasure of damaging information, and even to sue for damage caused by inaccurate information.

“Personal data” must not be kept for longer than is necessary, so emails should be stored in such a way that they can be easily identified, reviewed and archived when they are no longer needed. Please see further guidance in the Ascend Email Policy. If in doubt, you should seek guidance from a Schools Data Protection Lead (DPL), or Trust Data Protection Officer (DPO).

If any user receives an email where they were not the intended recipient and a concern therefore arises regarding a GDPR breach, this email should be forwarded to the Trust Data Protection Officer (dpo@dataprotection.education) or the Data Protection Lead in each school. A short explanation should be included in the forwarded email explaining the context. The Data Protection Officer will then investigate and take necessary steps.

More information about the use and operation of emails is contained within the Ascend Email Policy.

Social Media

Social Media and networking sites should be treated with extreme caution. The following applies to different user groups:

Students

Students are not permitted to use Social Media using Trust technology at any time, they should not attempt to communicate with Trust staff at any time using any form of Social Media.

Employees

Staff must never access personal social media and/or networking sites on any trust device.

All staff are reminded that use of social media at any time and in any context to make comments of a negative or inappropriate nature about the Trust, its School’s, its employees, students, clients, customers, suppliers or other business associates, which might damage the Trusts reputation or interests, the Trust reserves the right to investigate such actions through the disciplinary procedure.

Social media and networking sites such as Facebook, Twitter, LinkedIn etc. may be accessed on Trust provided equipment during the working day for Trust business purposes, by designated individuals only. Any inappropriate use of social media during working hours may give rise to disciplinary action.

When using social media for trust business, such as posting tweets or updates on Trust or School social media sites, then the followers and fans attracted to those sites are deemed to be followers and fans of the Trust or School, not of an individual user. If a designated individual leaves the Trust's employment, they must not continue to use the same account or give the impression that they are still a Trust representative.

Designated individuals are also reminded that any social networking activities they conduct on Trust equipment must be lawful and appropriate and not in any way defamatory, malicious or likely to damage the reputation of the Trust.

Protection from Cyber Attacks

Please see the glossary (appendix 4) to help you understand cyber security terminology.

The Trust will:

- Work with Trustees, the executive leadership team, governors and the IT Support teams to make sure cyber security is given the time and resources it needs to make the Trust secure.
- Provide annual training for staff (and include this training in any induction for new starters if they join outside of the Trust's annual training window) on the basics of cyber security.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.
- Ensure that internet safety and safe use of the internet, including an awareness of cyber attacks, is part of the PSHE curriculum and will be delivered to students in a relevant way.
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.

Put controls in place that are:

- **Proportionate**: the Trust will verify this using a third-party audit (such as independent penetration testing, to objectively test that what it has in place is effective
- **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- **Up to date:** with a system in place to monitor when the Trust needs to update its software
- **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be

- Back up critical data daily, weekly, monthly and yearly.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to data manager / business managers within schools, and the Trust IT Lead
- Have firewalls in place, that are actively monitored
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification.
- Develop, review and test an incident response plan with IT Support including, for example, how the Trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually. and after a significant event has occurred, using the NCSC's 'Exercise in a Box'.

Make sure users:

- Connect to our network using the authorised methods from each school
- Enable multi-factor authentication where possible
- Connect to Wi-Fi solutions using account authentication so that device access is auditable

More information about Cyber Security is contained within the Ascend Cyber Security Policy.

Telephones and Voicemail

Telephones should be answered in a friendly but professional manner, and as promptly as possible. Trust telephones are principally provided for business purposes and under no circumstances should premium rate numbers be called, at any time. Specific guidance should be sought from individual headteachers and/or the executive leadership team if a need arises to place an overseas phone call.

When leaving voicemail messages, you should follow the same rules of professionalism that guide the use of e-mail.

From time to time, it may be necessary for students to use trust telephones, such as to contact a work experience placement provider or to make contact with a parent/carer in an exceptional circumstance. In such instances, telephone calls should be supervised.

AI (Artificial Intelligence)

The Trust permits the informed and responsible use of authorised AI applications, in carrying out specific and authorised tasks. Please see the Ascend AI Policy for more information.

Ascend schools may permit pupil usage of AI in the following circumstances:

- As a research tool
- Idea generation for projects
- Revision aids

- Development of critical thinking skills

Examples of AI misuse include, but are not limited to, the following:

- Copying or paraphrasing sections of AI-generated content so that the work is no longer the pupil's own
- Copying or paraphrasing whole responses of AI-generated content
- Using AI to complete parts of an assessment or homework so that the work does not reflect the pupil's own work, analysis, evaluation or calculations
- Failing to acknowledge use of AI tools when they have been used as a source of information
- Incomplete or poor acknowledgement of AI tools
- Submitting work with intentionally incomplete or misleading references

Employees may utilise AI to support the planning of teaching and learning activities.

Misuse of AI tools, or any other failure to comply with this policy will be investigated through an appropriate policy depending on the user group.

Misrepresentation or Misuse of Technology

When using any Trust-provided communication tool, individual users are reminded that they represent the Trust. Email or internet messages can be traced back to the Trust as their source. Therefore, individual users must exercise caution to protect the reputation and interests of the Trust.

Electronic forgery (misrepresenting your identity in any way while using electronic communication systems) is not allowed for any reason. Users may not take any action to misrepresent the identity of the person responsible for a message. If you forward a message prepared by someone else, it should be sent "as is," or if changes are necessary, users must clearly indicate where the original message was edited e.g. by using brackets, asterisks, or other characters to flag edited text.

Users are also reminded to be vigilant about receiving communication where others may be misrepresenting themselves. Therefore, users should be wary of electronic communication from unknown people.

Misuse of communication tools may interfere with business operations and may injure the Trust or other employees. As a general rule, individual users should not create or send any message, using any technological medium, that they would not want an outside party to view. A good test is whether they would be happy to see this on the front page of the local newspaper, and if the answer is no, then the message is probably not appropriate.

Examples of unacceptable use of technology include (This list is not exhaustive):

- Sexually explicit messages, images, cartoons or jokes
- Unwelcome propositions, requests for dates or love letters
- Profanity, obscenity, slander or libel

- Expressions of political beliefs
- Derogatory, defamatory, threatening, abusive, rude or offensive language
- Any message that could be construed as harassment or disparagement of others based on sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs
- Commercial or for-profit activities unrelated to Trust operations
- Chain letters
- Excessive use of the technology for personal purposes
- Release of confidential, sensitive or proprietary information
- Gambling including accessing explicit gambling sites, or using technology to access third party sites associated with gambling activities.
- Any action that is illegal or harmful to the Trust or any School.

Misuse of Trust-provided technological tools, or any other failure to comply with this policy will be investigated through an appropriate policy depending on the user group, including disciplinary or behaviour policies.

The following section is only applicable to employees of the Trust.

Confidential information

In order to perform their job responsibilities, employees are given access to confidential data that is vital to Trust operations. In such circumstances, users must respect the confidentiality of such data.

Because of the highly public nature of the Internet and email, users must exercise particular care when accessing or transmitting information via those channels.

Removal of any Trust information for any reason without the express prior permission of the School Data Protection Lead or Data Protection Officer is prohibited.

Employees are also reminded that they should not access the confidential information of another member of the trust without a justified reason (such as accessing a telephone number of a next of kin in an emergency.)

Copyrighted work

Use of trust provided communication tools to access copyrighted materials is permitted. However, responsibility to ensure that copyrighted materials are not downloaded or shared rests with the individual user. Caution should be exercised when accessing copyrighted materials and particular attention should be paid when using video based resources accessed via streaming services.

At no time should personal accounts for services such as Netflix, Disney Plus, Amazon Prime and so on be used on a trust provided device.

Appendix 1 Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

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

The Trust uses the following channels:

- Our official Social Media Pages
- E-mail/Text groups for Parents (for School / Trust announcements and information)
- Various Learning Platforms (School specific)

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 Trust via official communication channels, or using private/independent channels to talk about the Trust, I will:

- Be respectful towards members of staff, the Trust, and its School's, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the Trust's official channels, so they can be dealt with in line with the Trust's complaints procedure I will not:
- Use private groups, the Trust's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the Trust can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the Trust's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the Trust 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 the other children's parents/carers

Signed:

Date:

Appendix 2 Acceptable use of the Trust's ICT facilities and internet: Agreement for pupils and parents/carers

Acceptable use of the Trust's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the Trust's ICT facilities and accessing the internet in Trust, whether on a Trust device or personal device, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break Trust rules
- Access any inappropriate websites
- Attempt to circumvent filtering and safeguards in place around Internet use
- 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 any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the Trust's network using someone else's details
- Bully other people

I understand that the Trust will monitor the websites I visit as part of my use of the Internet, using both Trust ICT facilities and systems as well as personal devices.

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's ICT systems and internet responsibly.

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

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the Trust's ICT systems and internet when appropriately supervised by a member of Trust staff.

I agree to the conditions set out above for pupils using the Trust's ICT systems and internet, and for using personal electronic devices in Trust, and will make sure my child understands these.

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

Appendix 3 Acceptable use of the Trust's ICT facilities and the internet: Agreement for Staff, Trustees, LAB Members, Volunteers and Visitors

Acceptable use of the Trust's ICT facilities and the internet: agreement for Staff, Trustees, LAB Members, Volunteers and Visitors

Name of Staff, Trustees, LAB Members, Volunteers and Visitors:

When using the Trust's ICT facilities and accessing the internet services provided by the Trust, in or outside of the Trust on a work device, or making use of Wi-Fi services on a personal 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's reputation
- Access social networking sites or chat rooms, unless for agree Trust or School business purposes
- 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's network
- Share my password with others or log in to the Trust's network using someone else's details
- Share confidential information about the Trust, its 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

I understand that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems, and that when using a personal device, my Internet usage will be tracked against my unique system credentials.

I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside the Trust, 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 Trust IT Support know if a 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's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (Staff, Trustees, LAB Members, Volunteers and Visitors):	**Date:**

Appendix 4 Glossary of cyber security terminology

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
TERM	**DEFINITION**
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multifactor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.