The

MAST

Academy Trust

Policy	ICT and internet acceptable usage policy
Owner	CFO
Date approved	20th March 2024
Approver	Finance, Audit & Risk Committee

Current version	V3.0
Next review due	Spring 2027

Objective of Policy

This policy aims to:

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

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

Version Control	
Version Number	Summary of amends from previous version
2.0	Amalgamation of acceptable usage and communication guidance into one policy.
3.0	Every 3-year review: Update to sections 2,3,4,5,6,7,8,9,10,11, appendix A, B & E.

Sign off requirements	
Approvers	Position
Finance, Audit & Risk Committee	Trust Board
Reviewers	Position
Jason Field	CFO
Ben Lunt	Trust representative

1. Introduction and aims

ICT is an integral part of the way The Mast Academy Trust works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the trust/ school.

However, the ICT resources and facilities our trust uses also pose risks to data protection, online safety and safeguarding.

This guidance is provided to protect trust and school staff from harassment, real or alleged misuse and any consequential disciplinary action arising from the use of electronic communication equipment in or outside school. It is also intended to ensure that the school's equipment is used responsibly and safely at all times. There are implications for the actions of individuals and the school as a whole.

This document is part of the trust and school's Information Security and Online Safety Policy.

Breaches of this policy may be dealt with under our:

- disciplinary policy
- behaviour policy
- staff code of conduct

Policies can be found on the Trust and school websites.

2. 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 2023
- Searching, screening and confiscation: advice for trust/ schools

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Types of communication":** include (but is not limited to) internet, telephone, email, text messaging, multimedia messaging, transmission of photographs and videos, contact via websites and social networking sites, blogging, wikis, contact via web cameras and internet phones, communication via tablet or smartphone apps.

- **“Users”:** anyone authorised by the trust/ / school to use the ICT facilities, including governors, trustees, staff, pupils, volunteers, contractors and visitors
- **“Personal use”:** any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”:** employees authorised by the trust/ / school to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the trust / school’s ICT facilities by any member of the trust / school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the trust / school’s ICT facilities includes:

- Using the trust / school’s ICT facilities to breach intellectual property rights or copyright
- Using the trust / school’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust / school’s 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 / school, or risks bringing the trust / school into disrepute
- Sharing confidential information about the trust / school, its pupils, or other members of the trust / school community
- Connecting any device to the trust / school’s ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the trust / school’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT 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 trust / school’s ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing credentials (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 / school

- Using websites or mechanisms to bypass the trust/ school's filtering mechanisms

This is not an exhaustive list. The trust / school reserves the right to amend this list at any time. The headteacher or CFO will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the trust / school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of trust / school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the CEO / Headteacher's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the trust's policies on:

- disciplinary policy
- behaviour policy
- staff code of conduct

Policies can be found on the Trust and school websites.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to trust / school ICT facilities and materials

The Trust's ICT collaborative provision manages access to the trust and school's ICT facilities and materials for 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/school's ICT facilities.

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 ICT collaborative teams.

5.1.1. The internet

The internet is a valuable work resource, which enriches teaching and learning. In school hours staff are expected to restrict internet access to work related activities. Reasonable personal use may be permitted outside recorded working time (for example at lunchtime).

Staff must not use electronic equipment for any form of illegal activity, e.g. downloading copyrighted material, introducing a virus, hacking into other computers, viewing or downloading pornographic, obscene, offensive, gambling or any other inappropriate material from any source, transmitting or storing such material on a computer. Criminal proceedings may result if any equipment is used for illegal activity, regardless of whether it is personal or school owned.

Action to take if you inadvertently access inappropriate material

- Staff inadvertently accessing inappropriate material should immediately inform the Headteacher or designated person in school and ensure that the incident is recorded in the online safety incident log.

5.1.2 Use of phones and email

The trust / school provides each member of staff 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 / school has provided.

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

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.

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. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

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 CFO immediately and follow the trust's data breach procedure.

The sending of abusive, threatening, discriminatory or other offensive email is forbidden and may be considered a criminal act. Bear in mind that emails may be submitted as evidence in legal proceedings and that email discussions with third parties can constitute a legally binding contract.

Email attachments should be opened with care unless you have absolute confidence in its origin as this is one of the most likely points of introducing a virus into a computer system.

An individual should not access the email of another individual within the school without express permission and a clear understanding of the reason for the proxy access.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the trust / school to conduct all work-related business.

Trust / school 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 ICT acceptable use as set out in section 4.

Action you must take if in receipt of inappropriate emails

- It is impossible to control what information is sent to a member of staff by email. However if offensive, obscene and/or discriminatory material is received it is then the responsibility of the receiver to report immediately, and in writing, to the designated person in school or the headteacher. Never send a reply.

- Keep a printed copy of the email as evidence and pass a copy of the email to the appropriate person for the record. Ensure that the sender's information is also recorded as their email service provider may take action.

- Do not forward any email containing a 'sexting' image of a child, even for investigation purposes. It is illegal to distribute indecent images of children, even if the image was originally created by the child themselves.

5.2 Personal use

5.2.1 Use of equipment

Staff are permitted to occasionally use trust / school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The CEO/Headteacher 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 contact time/teaching hours/non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the trust / school's ICT 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 / school's ICT facilities for personal use and personal communications within the scope of the trust/ school's ICT monitoring activities (see section 5.6). 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 / school's Information Security Guidance for Staff Policy.

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

Staff should take care to follow the trust / school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.2 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 / school has guidelines for staff on appropriate security settings for social media accounts (see appendix A).

Staff should not use trust and school facilities to access or update personal social networks. Staff should be aware of the potential risk to their professional reputation and potential for safeguarding allegations caused by adding pupils/students, parents or friends of pupils/students to their social network contacts and are strongly recommended not to do so.

Care should be taken that comments made on a social network site, website or app do not relate to or identify the school, staff or pupils as this could result in disciplinary action. It is also important that photographs and descriptions of activities in the personal life of staff do not adversely affect the professional reputation of staff or the school. Staff should be aware that

even if they have used the privacy settings, they may not be able to prevent material becoming public due to the risk of republishing by someone else.

It is recognised that online social communications tools, such as blogs and wikis, have a potentially useful role in schools – such as on school websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where pupils and their families are sharing these tools with staff in school it is important that this should always be through a school based resource, such as the school Learning Platform, using a school account where all communication is open and transparent.

If a member of staff keeps a personal blog the content must maintain acceptable professional standards. Any inappropriate use may lead to disciplinary action in accordance with school policy. All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school.

Schools are vulnerable to material being posted about them online and all staff should report this should they become aware of anything bringing the school into disrepute. School will regularly check using a search engine whether any such material has been posted.

Action you must take if you discover inappropriate, threatening or malicious material online concerning yourself or your school:

- Secure and preserve any evidence. For example, note the web address (URL) or take a screen shot or copy and print the screen
- Report immediately to your line manager or headteacher, who will investigate the incident
- After investigation, contact the uploader of the material or the Internet Service Provider/ website administrator and ask for the material to be removed.

All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others. If the material has been created by a pupil or staff member then the school have a responsibility to deal with it. Illegal material which is discrimination, hate crime or a credible threat of violence needs to be reported to the police.

5.3 Real time online communication

The ability to communicate using voice, text or webcams in real time using the computer, tablet devices and mobile phones makes these an excellent tool for a range of educational purposes. However, staff should take the same level of care with these tools as they would if working in a face to face situation with a pupil/student or group of pupils/students. Access should always be through a school created account, never a personal account and it should be focused on a clearly specified educational objective.

There may be times when this kind of activity will happen outside normal school hours and off the trust and school premises. In this situation it should always be carried out with the full knowledge and agreement of a line manager. Staff should be aware that they must remain focused on the educational purpose of the communication and never allow it to become a social exchange.

Staff should also agree to specific times for availability and only allow contact during these times, to protect their personal time. When a web camera is used it should have a clear purpose. Staff should be aware of the ability of meetings of this kind to be recorded without their knowledge. However, they may wish to use this function for their own security, as long as all parties are informed that recording is taking place.

Staff must protect their privacy by never allowing pupils or parents to obtain their personal contact details such as a mobile phone number or email address. Online bullying of staff by pupils is possible by mobile phone or email.

Action you must take if an incident occurs

- Report immediately and in writing to your line manager.
- Don't reply to abusive or worrying text or video messages.
- Don't delete messages. Keep them for evidence.
- Try and obtain the phone number if you can. Most calls can be traced.
- Report it to your phone provider and/or request a change of number
- Technical staff may also be able to help you to find or preserve evidence e.g. logs of the call.

5.4 Remote access

We allow staff to access the trust / school's ICT facilities and materials remotely by use of the ICT equipment provided.

Staff accessing the trust / school's ICT 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 / school's ICT facilities outside the trust / school and take such precautions, as the CFO may require from time to time, against importing viruses or compromising system security.

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 our Data Protection policy and Information Security Guidance Policy.

5.5 Trust/ school social media accounts

The trust / school has official social media pages, including but not limited to: Facebook and X (formerly twitter). 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 / school 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.

5.6 Monitoring of trust / school network and use of ICT facilities

The trust / school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- Video conferencing calls
- User activity/access logs
- Any other electronic communications

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

The trust / school monitors ICT use in order to:

- Obtain information related to trust / school business
- Investigate compliance with trust / school policies, procedures and standards
- Ensure effective trust / school and ICT 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

6. Pupils

6.1 Access to ICT facilities

ICT facilities are available to pupils, under the following circumstances:

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment
- Computers and equipment may be loaned to pupils, as required, with permission of the headteacher

6.2 Search and deletion

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

The school 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 school's rules.

6.3 Unacceptable use of ICT and the internet outside of trust / school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust / school's 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 / school, or risks bringing the trust / school into disrepute
- Sharing confidential information about the trust / school, other pupils, or other members of the trust / 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 / school's ICT facilities

- Causing intentional damage to ICT 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

Refer to section 4.2 for sanctions.

Further guidance can be found in the school's Online Safety Policy.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the trust / school's ICT facilities as a matter of course.

However, parents working for, or with, the trust / school 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 / school's facilities at the CEO / Headteacher's discretion.

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

7.2 Communicating with or about the trust / school online

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

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

We ask parents to sign the agreement in appendix B.

8. Data security

The trust / school takes steps to protect the security of its computing resources, data and user accounts. However, the trust / school cannot guarantee security. Staff, pupils, parents and others who use the trust / school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the trust / school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users must follow the Information Security Guidance Policy.

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

8.2 Software updates, firewalls, and anti-virus software

All of the trust / school's ICT 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 / school's ICT facilities.

Any personal devices using trust / school's network must all be configured in this way.

Users must follow the Information Security Guidance Policy.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the trust / school's data protection policy.

8.4 Access to facilities and materials

All users of the trust / school's ICT facilities will have clearly defined access rights trust / school systems, files and devices.

Users must follow the Information Security Guidance Policy.

8.5 Encryption

The trust / school ensures that its devices and systems have an appropriate level of encryption.

Users must follow the Information Security Guidance Policy.

9. Internet access

The school's wireless internet connection is secured.

Access to, and permission to access, the school Wi-Fi must be obtained from the ICT team in school prior to connection

9.1 Pupils

Access to, and permission to access, the school Wi-Fi by pupils must be obtained from the ICT lead in school prior to connection.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with the trust / school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10.0 Expectations of the trust and school

In order to ensure safe practice for staff, the trust and school should:

- Make it clear that the trust and school will enforce policies to protect staff and pupils from malicious use of mobile phones, in particular the use of camera and video functions on phones
- Ensure that the school's policy and procedures for home-school communication are shared with all staff
- Establish whole trust and school systems for: storing emails, dealing with inappropriate messages and breaches of security
- Provide all staff and members of governing bodies with a trust email address to be used

for all school-related communications

- Establish clear ICT policies for monitoring use of the school's electronic equipment by staff, including procedures for accessing email and files when staff are absent due to holiday, illness, etc
- Provide digital cameras and mobile phones which can be borrowed by staff as required for all school-related work
- Provide a safe learning environment with appropriate filtering and monitoring and approved online tools for electronic communications with pupils
- Ensure there are established systems for reporting unwanted or accidental electronic communications and that staff know who the correct person to report any issues to is. Ensure these are correctly recorded. Treat such incidents seriously.
- Regularly check the trust and school's presence on the internet to ensure material detrimental to the trust or school is identified quickly.

11. Monitoring and review

The Headteacher and CFO monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the trust / school.

This policy will be reviewed every 3 years.

12. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Information security

Appendix A: Social media guidance for staff

Don't accept friend requests from pupils on social media

10 tips for trust/ and school staff on social media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during trust / school hours
7. Don't make comments about your job, colleagues, the trust / school or pupils online – once it's out there, it's out there
8. Don't associate yourself with the trust / school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a trust / school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the social media apps from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos**
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name**
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the trust / school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix B: 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 / school. The trust / school uses the following channels: Social media including, but not limited to: Our official Facebook page; Our Twitter account • Email/text groups for parents (for trust/ school announcements and information) • Our virtual learning platform • Communication platforms • Websites 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 / school via official communication channels, or using private/independent channels to talk about the trust / school, I will: • Be respectful towards members of staff, and the trust / school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the trust / school's official channels, so they can be dealt with in line with the trust/ school's complaints procedure I will not: • Use private groups, the trust / school's Social Media Platforms, or personal social media to complain about or criticise members of staff. This is not constructive and the trust / school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the trust / school's Social Media Platforms, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the trust / school 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	
Signed:	**Date:**

Appendix C: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for older pupils and parents/carers	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, 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 school rules • Access any inappropriate websites • Access social networking sites (unless my teacher 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 school's network using someone else's details • Bully other people **When using the school's ICT facilities and accessing the internet in school, I will:** • Take care when using school IT equipment and use it responsibly • Immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others • Always use the school's ICT systems and internet responsibly I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. 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 school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT 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 school's ICT 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 school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix E: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the trust/ school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the trust / school's ICT facilities and accessing the internet in the trust / school, or outside the trust / school 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 / school's 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 / school's network • Share my password with others or log in to the trust / school's network using someone else's details • Share confidential information about the trust / school, 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 / school	
I understand that the trust / school will monitor the websites I visit and my use of the trust / school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the trust / school, and keep all data securely stored in accordance with this policy, the information security policy and the data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager 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 / school's ICT systems and internet responsibly and ensure that pupils in my care do so too. I will follow the Information Security Policy, Data Protection Policy and ICT and Internet acceptable use Policy as required by my role.	
Signed (staff member/governor/volunteer/visitor):	**Date:**