ICT AND INTERNET ACCEPTABLE USE POLICY

Drafted by:	Ellena Skoulding
Version Number:	V1.3
Status and Review Cycle	Statutory and Bi-Annual
Date Approved:	13th May 2026
Signed by **Chair of Trustees:**	 Ruth Slater

Trust Address:

64 Prince of Wales Drive

Ipswich

IP2 8PY

Registered in England and Wales, Company Number: 10650092

Policy Updates

Version	Date	Description of Changes	Initials
V1.3	13/05/2026	Added section 5.6 on email retention	ES

Contents

1. Introduction and aims:

ICT is an integral part of the way our schools work, and is a critical resource for pupils, staff, trustees, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

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

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 our school communities engage with each other online.
- Support the trust's policy on data protection, online safety and safeguarding.
- Prevent disruption to the schools and the trust through the misuse, or attempted misuse, of ICT systems.
- Support the schools in teaching pupils safe and effective internet and ICT use

This policy covers all users of our Trusts ICT facilities, including trustees, governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Staff Disciplinary Policy.

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
- Searching, screening and confiscation: advice for 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.
- "Users": anyone authorised by the academy trust to use the ICT facilities, including trustees, governors, 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 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 academy trust's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the academy trust's ICT facilities includes:

- Using the academy trust's ICT facilities to breach intellectual property rights or copyright.
- Using the academy trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the academy trust'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 academy trust, or risks bringing the academy trust into disrepute.
- Sharing confidential information about the academy trust, its pupils, staff or other members of the academy trust's community.
- Connecting any device to the school's/ academy trust's ICT network without approval from authorised personnel.
- Setting up any software, applications or web services on the school's/ academy trust'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 academy trust'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 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 academy trust.
- Using websites or mechanisms to bypass the academy trust's filtering mechanisms.

This is not an exhaustive list. The academy trust reserves the right to amend this list at any time. The Headteacher at each school and CEO/CFO for the Shared Services Team, will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy trust's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of academy trust ICT 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 headteacher within each individual school and by the CEO/CFO for the Shared Services Team.

Staff should consult the Headteacher for schools and CEO/CFO for the Shared Services Team, on how and why they intend to use academy trust's IT facilities. If permission is given, the decision will be recorded and kept on electronic file.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy trust's policies on Behaviour, Staff Code of Conduct or Staff Discipline. Trustees, Governors, and volunteers who engage in any of the unacceptable activity listed above may be dismissed.

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

5.1 Access to academy trust ICT facilities and materials

Each school's Office Manager and the CFO for the Shared Services Team, along with Technical Support, will manage access to each school's and Shared Services Team ICT facilities and materials for academy trust 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 academy trust'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 their Office Manager.

5.1.1 Use of phones and email

The academy trust provides each member of staff, trustees and governors with a Trust email address which gives them access to the suite of Office tools on Microsoft 365.

This email and office account should be used for work purposes only.

All work-related business should be conducted using the email address the academy trust 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. Where possible personal/sensitive data should be shared via a link. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. Email accounts must not be used to store information.

All Senior Leaders, SENCos, DSLs/ADSLs and Office Managers have been provided with an individual secure SharePoint for sending sensitive or confidential documents to people/ organisations outside of the academy trust.

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 inform their school's / team's Data Protection Lead and 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 their Headteacher for school-based staff and CEO/CFO for Shared Services based staff immediately and follow our data breach procedures (see GDPR policy).

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the academy trust or an individual school's/ Shared Services Phone app to conduct all work related business.

Academy Trust phones must not be used for personal matters unless permission has been given by the Headteacher/CFO/CEO.

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.

5.2 Personal use

Staff are permitted to occasionally use academy trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher/CFO/CEO 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 the school day.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils or parents 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 academy trust'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 academy trust's ICT facilities for personal use may put personal communications within the scope of the academy trust's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones/ tablets or smart watches) to access school related apps such as Microsoft 365, Class Dojo and Arbor, as long as no confidential information is download/ screenshotted and saved on the device.

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

Staff should take care to follow the 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.

5.2.1 Personal social media accounts

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

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

Refer to the OMAT Social Media policy for more information.

5.3 Remote access

We allow technical staff to access the academy trust's ICT facilities and materials remotely.

The School's Technical Support Manages this access.

Support use Team Viewer as their host.

Remote access is not granted to members of academy trust staff beyond technical support.

Technical Support accessing the academy trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. They must be particularly vigilant if they use the academy trust's ICT facilities outside the academy trust and take such precautions as may be required 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.

5.4 School social media accounts

The academy trust has an official Twitter page as well as some individual school Twitter/Facebook/Instagram pages. Arrangements for managing these are agreed at individual school/setting level with senior staff oversight. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The 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 always abide by these guidelines.

For example, only children with adequate internet permissions may appear. Staff must not use their personal devices to take photographs of pupils to upload to social media.

5.5 Monitoring of school network and use of ICT facilities

The academy trust 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.
- User activity/access logs.
- Any other electronic communications.
- Only authorised ICT staff may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The academy trust monitors ICT use in order to:

- Obtain information related to school business.
- Investigate compliance with academy trust policies, procedures and standards.
- Ensure effective school/shared services team 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.

Our trust board is responsible for making sure that:

- The schools meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place

- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The schools' designated safeguarding leads (DSLs) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the appropriate schools' DSL and ICT manager, as appropriate.

5.6 Email Retention

Recent Subject Access Requests (SARs) have required us to review email accounts in detail. This has highlighted that emails are often being retained for longer than necessary.

Under the UK GDPR and the Data Protection Act 2018, personal data must only be kept for as long as needed for its original purpose. Once a SAR is received, it becomes a criminal offence to delete any data that would not have been removed as part of normal retention processes.

It is also important to note that email accounts can be vulnerable to hacking. Retaining unnecessary emails increases the amount of sensitive information at risk in the event of a security breach.

What staff need to do:

1. Regularly delete emails that are no longer required
2. Save emails needed long-term to the school network or the school Management Information System as appropriate
3. Move short-term emails into a dedicated folder with a clear "destroy date" in the folder name.

Important upcoming change:

From 1 September 2026, emails older than 2 years will be automatically deleted. Please ensure that any emails dated before 31 August 2024 that still need to be kept are saved in the appropriate location before this deadline.

Tip for file naming:

Use the format **YY.MM.DD** at the start of file names (e.g. 26.04.28 for 28 April 2026). This keeps files in chronological order and makes it easier to identify the latest version

6. Pupils

6.1 Access to ICT facilities

Academy trust computers and equipment 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.

All pupils are provided with a Google Classroom login. In some schools, children are also given accounts for other software such as Purple Mash, TT Rockstars and Accelerated Reader.

Passwords are unique to each child. Children are regularly reminded not to share their passwords with anyone else.

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 academy trust has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under academy trusts rules or legislation.

The academy 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 trust's rules.

6.3 Unacceptable use of ICT and the internet outside of school

Each school will sanction pupils, in line with their 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 academy trust'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 academy trust, or risks bringing the academy trust into disrepute.
- Sharing confidential information about the academy trust, other pupils, staff, 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 academy trust'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.

6.4 Ensuring Internet Access is Appropriate and Safe

The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

Our Internet access is purchased from Coconnect which provides a service designed for pupils including a filtering system intended to prevent access to material inappropriate for children;

Netsupport is used to monitor the activity pupils are undertaking on all devices across all programmes. The headteacher and/or DSL uses this to monitor the activity across their school's IT infrastructure;

- Children using the Internet will normally be working during lesson time and will be supervised by an adult at all times;
- Staff will check that the sites pre-selected for pupil use are appropriate to the age of the pupils;
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;
- Pupils will be taught to use the Internet responsibly in order to reduce the risk to themselves and others;
- Each schools' ICT lead will monitor the effectiveness of Internet access strategies;
- Each schools' ICT lead will ensure that random checks are made on files to monitor compliance with the school's ICT Acceptable Use Policy;
- Each headteacher will ensure that the policy is implemented effectively through regular review;

- pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable and all sites will be immediately reported to the IT provider to be blocked.

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the academy trust 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 academy trust's facilities at the headteacher's/CFO's/CEO's discretion.

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

Where schools use Class Dojo, parents are given access to support their child's home learning and to engage in class activities. Contributions to the Class Dojo are monitored by Class teachers and Senior Leaders within each school. Any inappropriate contributions will be reported to the individual school's Headteacher and may result in access being denied (see Class Dojo Policy).

7.2 Communicating with or about the 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 schools/academy trust through our websites and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

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

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure and not share with anyone else. Email accounts should have a strong unique password.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Pupils have their passwords for Purple Mash, TT Rockstars, Accelerated Reader and Google Classrooms randomly generated. In some schools, single sign ins are being developed, so children have one password and login for all the websites they use.

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.

Staff should update their passwords at least every six months using a combination of: Upper case letters, lower case letters, numbers and symbols. Passwords must be at least twelve characters long. The National Cyber Security Centre recommends using 3 random words.

8.2 Software updates, firewalls, and anti-virus software

All of the academy trust'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 academy trust's

ICT facilities.

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

8.3 Data protection

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

8.4 Access to facilities and materials

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

These access rights are managed by our IT technicians and the Office Manager.

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 the Headteacher or CFO immediately.

Users should always log out of systems and lock their equipment when they are not in use 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.

8.5 Encryption

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

School staff may only use personal devices to access school data, work remotely, if they have been specifically authorised to do so by the headteacher. Personal USB drives are strictly forbidden.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the academy trust's Technical Support, Headteacher/CFO or CEO.

Academy trust staff may only use Cloud Based Storage services that have been provided by the school (such as Microsoft 365 and Google Drive for Google Classrooms) to store academy trust data and personal data as these systems have encryption and password security at the approved level.

9. Internet access

Wireless internet connections across all academy trust sites are securely filtered and the access code updated every six months.

Filtering is not fool-proof. If staff, parents, visitors or pupils identify that inappropriate content is being or could be viewed, they must inform the Office Manager or Headteacher immediately so that the filters can be updated.

If staff are using Academy trusts ICT equipment at home, it is advisable that they change the default usernames and passwords for their home wi-fi router, as these are often publicly available on the Internet and can leave Academy trust ICT equipment vulnerable to hackers, who could access files and introducing viruses and malware.

9.1 Pupils

Pupils can only access the internet under the supervision of a member of academy trust staff.

9.2 Parents and visitors

Parents and visitors to each of the academy trust's schools 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 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. Monitoring and review

The headteacher and Office Manager in collaboration with the academy trust's technical support monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the schools and shared services team.

This policy will be reviewed every two years.

The Trust Board is responsible for approving this policy for use in each school/setting within the Trust.

11. Related policies

This policy should be read alongside the academy Trust's and individual school's policies on:

- Online Safety
- Safeguarding
- Behaviour
- Staff Discipline/Code of Conduct
- Data Protection/GDPR
- Social Media Policy
- Class Dojo Policy

Appendix 1: Social Media cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for academy trust 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 school hours
7. Don't make comments about your job, your colleagues, your school or your pupils online – once it's out there, it's out there.
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a 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 Facebook app 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** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts.

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** – go to bit.ly/2zMdVht to find out how to do this.

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 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 Facebook or 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 2: 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 school. The school uses the following channels: • Our official Twitter account • Email/text groups for parents (for school announcements and information) • Class Dojo 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 school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, 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 school's Twitter page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the 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 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for 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 the school's network using someone else's details • Bully other people I understand that the school will monitor the websites I visit and my use of the school's ICT 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 school's ICT systems and internet responsibly. 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 4: Acceptable use agreement for younger pupils

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 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/trustee/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside 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 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 school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the 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 school
- Click on links from external emails without checking their authenticity.
- Leave equipment in vehicles overnight.

I understand that the school will monitor the websites I visit and my use of the 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 inside and outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. This includes:

- Locking screens when not in use to avoid any unauthorised access.
- Logging out and shutting down equipment and systems at the end of the day.
- Having a strong unique password for my email account.
- Activating Multi Factor Authentication on accounts where available.

I will let the Headteacher - designated safeguarding lead (DSL) and Office 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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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