



IT - Acceptable Use Policy

Mercian Educational Trust

Inspire to Aspire

Author:- DLawday@metacademies.org.uk

**Agreed
on:-**

**Ratifying
Group:-**

**To be
reviewed:**

**MET
Executive
Team**

01/09/2026

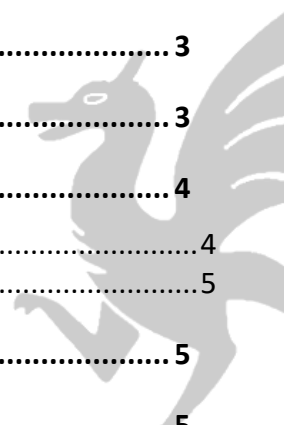
AMENDMENTS TO POLICY

<i>Item</i>	<i>Location</i>	<i>Date of change</i>	<i>By</i>
<i>Changed responsibility to Trust Executive</i>	<i>n/a</i>	<i>September 2023</i>	<i>CEO</i>
<i>Removed references to Twitter replaced with Instagram.</i>	<i>0</i>	<i>September 2024</i>	<i>CEO</i>
<i>Removed reference to all classes have social media accounts</i>	<i>0</i>	<i>September 2024</i>	<i>CEO</i>
<i>Changed identified support and technical providers</i>	<i>Throughout</i>	<i>October 2024</i>	<i>CEO</i>
<i>General review and update Exchanged references to Scholarpack with Arbor and retired Appendix 5 glossary in favour of online glossary from NCSC</i>	<i>Throughout</i>	<i>September 2025</i>	<i>CEO</i>

Contents

1. Introduction and aims.....	4
2. Relevant legislation and guidance	4
3. Definitions	5
4. Unacceptable use.....	5
4.1 Exceptions from unacceptable use	6
4.2 Sanctions	6
5. Staff (including governors, volunteers, and contractors)	6
5.1 Access to school ICT facilities and materials	6
5.1.1 Use of phones and email	7
5.2 Personal use	7
5.2.1 Personal social media accounts	8
5.3 Remote access	9
5.4 School social media accounts	0

5.5 Monitoring of school network and use of ICT facilities.....	0
6. Pupils.....	0
6.1 Access to ICT facilities	0
6.2 Search and deletion	1
6.3 Unacceptable use of ICT and the internet outside of school	1
7. Parents	1
7.1 Access to ICT facilities and materials	1
7.2 Communicating with or about the school online	3
8. Data security	3
8.1 Passwords	3
8.2 Software updates, firewalls and anti-virus software	3
8.3 Data protection	3
8.4 Access to facilities and materials.....	3
8.5 Encryption	4
9. Protection from cyber attacks	4
10. Internet access	5
10.1 Pupils.....	5
10.2 Parents and visitors	5
11. Monitoring and review	6
12. Related policies	6
Appendix 1: Acceptable use of the internet: agreement for parents and carers	7
Appendix 2: Acceptable use agreement for older pupils	8
Appendix 3: Acceptable use agreement for younger pupils	9
Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors	10
Appendix 5: Glossary of cyber security terminology	Error! Bookmark not defined.



Mission:

"Empowering pupils and employees to develop a range of diverse skills to thrive in an evolving world through our family of distinctive schools. "

Trust Values

Empowering our community to develop a range of diverse skills to thrive in an evolving world through our family of distinctive schools



We are prepared;
our staff, equip our
pupils for a
successful future.



We are empowered;
we work together to
encourage each
other's unique
strengths and
ambitions.



We thrive in a safe
environment which
encourages our love
of learning.

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way schools within Mercian Educational Trust work. It is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

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

This policy aims to:

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

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

Breaches of this policy may be dealt with under our behaviour policy and staff code of conduct.

PLEASE NOTE:- September 2025 – April 2026 This policy applies to all MET Schools with exception of Grove Primary School, as the school has pre-conversion (July 2025) systems and contracts in place

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 2025](#)
- [Searching, screening and confiscation: advice for schools](#)
- [National Cyber Security Centre \(NCSC\)](#)
- [Education and Training \(Welfare of Children Act\) 2021](#)

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 Trust / school to use the ICT facilities, including 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

See the [NCSC glossary](#) for cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the school’s ICT facilities includes:

- ✳️ Using the school’s ICT facilities to breach intellectual property rights or copyright
- ✳️ Using the school’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- ✳️ Breaching the school’s policies or procedures
- ✳️ Any illegal conduct, or statements which are deemed to be advocating illegal activity
- ✳️ Online gambling, inappropriate advertising, phishing and/or financial scams
- ✳️ Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- ✳️ Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- ✳️ Activity which defames or disparages the school, or risks bringing the school into disrepute
- ✳️ Sharing confidential information about the school, its pupils, or other members of the school community
- ✳️ Connecting any device to the school’s ICT network without approval from authorised personnel
- ✳️ Setting up any software, applications or web services on the 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 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 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 school
- ✖ Using websites or mechanisms to bypass the school's filtering mechanisms
- ✖ Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

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

4.1 Exceptions from unacceptable use

Where the use of IT facilities (on a school premise and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Trust & School Leadership discretion.

Trust Central Staff and School Leaders should contact the CEO via email to obtain permission; school staff should contact their Headteacher before commencing the activity.

The request should state why the action is required and why it may be considered unacceptable use. Where an email may breach confidentiality / data protection the person should contact the CEO / Headteacher for an in-person discussion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour and staff code of conduct.

All relevant policies can be found within the Trust or School Policy library, accessible via Teams / SharePoint or on request at a school office.

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

5.1 Access to school ICT facilities and materials

The school Senior Administrator, with support from the Trust IT support provider, manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- ✖ Computers, tablets, mobile phones 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 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 Senior Administrator. Access to SharePoint / Teams data can also make a direct request to access files. Requests will be sent to the team owner.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the 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 that contains the personal information of another person, they must inform the Senior Administrator immediately and follow the data breach procedure.

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

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 4. Unacceptable use.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. Trust or School Leadership 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 4. Unacceptable use
- ❌ 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 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 school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). 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 school's personal device policy.

Staff should be aware that personal use of ICT (even when not using 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 school's guidelines on [social media](#) and use of email (see **5.1.1 Use of phones and email**) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times. Further details can be found in the [Social Media Policy](#)



5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely through the following secure Log in services. Staff accessing the 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 school's ICT facilities outside the school and take such precautions to prevent the import of 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](#).

What	Who Has Access	Who manages it	Security arrangements	Protocols for remote access	How staff can request remote access
Microsoft 365	All MET Pupils and Staff receive access to appropriate file storage areas	MET IT Teams Admin Access – School nominated personnel	Secure Log-In Access only to nominated areas MFA for users with admin access Security policies in place for students	Cloud based, access via browser	Contact Senior Admin
Arbor	Leaders Admin Teachers Support Staff	School Admin Trust Admin Arbor	Access to the MIS data is controlled via appropriate role allocation	Cloud based, access via browser	Contact Senior Admin
CPOMS	All School Staff receive access to the service	School Admin CPOMS	School Staff - log incidents and information only DSL personnel have access to view and respond submissions	Cloud based, access via browser	Contact Senior Admin
Hoge 100	Leaders, Business & Finance Team School Administrators	Trust Admin Hoge 100	Secure Log-In to nominated areas only	Cloud based, access via browser	Contact Trust CFO
IMP	Leaders, Business & Finance Team	Trust Admin IMP	Secure Log-In to nominated areas only	Cloud based, access via browser	Contact Trust CFO

5.4 School social media accounts

Each school and the Trust have an official Facebook & Instagram pages, managed by Trust / School Leadership.

Staff members who have not been authorised to manage, or post to, the accounts, must not access, or attempt to access them.

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 abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

Internet access using school devices is monitored through [Securus Software](#). The school subscribes to a full monitoring service.

The 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
- ✖ 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 school monitors ICT use in order to:

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

The following ICT facilities are available to pupils, when and under what circumstances.

- ✖ Computers and equipment - Are available to pupils only under the supervision of staff
- ✖ Specialist ICT equipment, such as that used for music, design and technology, or video editing - Must only be used under the supervision of staff
- ✖ Pupils will be provided with an account linked to the school's Microsoft 365 tenant, which they can access from any device by using the following URL www.office.com

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under 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.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

6.3 Unacceptable use of ICT and the internet outside of school

The 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 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
- 🚫 Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- 🚫 Activity which defames or disparages the school, or risks bringing the school into disrepute
- 🚫 Sharing confidential information about the school, other pupils, or other members of the school community
- 🚫 Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- 🚫 Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the 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

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with the 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 school's facilities at the 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 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 school through our website and social media channels.

We ask parents to sign the agreement in



8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

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

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

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.

All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

8.2 Software updates, firewalls and anti-virus software

All of the 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 school's ICT facilities.

Any personal devices using the school'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 school's [data protection policy](#).

8.4 Access to facilities and materials

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

These access rights are managed by the Trust IT technician and our 3rd line providers, D&D and Chestnut

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 Senior Administrator 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, or take personal data out of school if they have been specifically authorised to do so by the headteacher.

The use of USB storage devices is prohibited

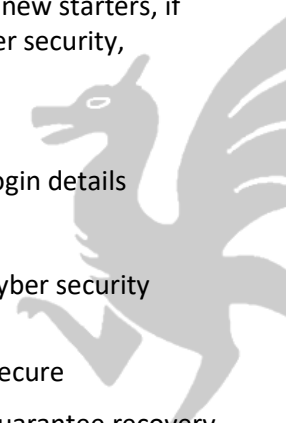
Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by Microsoft 365 and Trust IT technician

9. Protection from cyber attacks

Please see the [NCSC glossary](#) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- 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 [this one](#)), to objectively test that what it has in place is up to scratch
 - **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 school needs to update its software
 - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data automatically and daily and store these backups on [cloud based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises]
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Arbor (Nov 2024– onwards)
- Make sure staff:
 - Enable multi-factor authentication where they can, on things like school email accounts



- Store passwords securely using a password manager
- ✳️ Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- ✳️ Have a firewall in place that is switched on
- ✳️ Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the [Cyber Essentials](#) certification
- ✳️ Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify [Action Fraud](#) of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'
- ✳️ Work with Mercian Educational Trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school wireless internet connection is secured and filtered. However, the Trust acknowledges that no filter is fool-proof. In the event of a filter failure School Leaders must be notified immediately so that the filter service provider can be notified and modify filter parameters.

10.1 Pupils

Pupils are not provided access to the school Wi-Fi through their own devices.

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Trust or School Leadership.

They 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.



11. Monitoring and review

Monitoring of this policy will be conducted collaboratively between:

Trust Leadership

School Leadership

Senior Administrators

Together they will ensure it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The Trustees board is responsible for approving this policy.

12. Related policies

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

- Social Media
- Safeguarding and child protection
- Behaviour
- Codes of Conduct
- Data protection
- Remote learning



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/carers:

Name of child:

Online channels are an important way for parents/carers to receive information and news about our school.
The school uses the following channels for promotion and one way communication:

- Our official Twitter / Facebook page
- Website messaging App for parents (for school announcements and information)

The school also acknowledges and advocates parents/carers creating 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 social media pages, 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 social media pages, 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 2: 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 any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- 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/carers 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/carers):

Date:

Appendix 3: 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 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
- ☒ Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- ☒ 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/carers 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/carers):

Date:

Appendix 4: 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/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

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 outside school, and keep all data securely stored in accordance with this policy and the school's 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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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

Date: