IT Acceptable Use Policy

Version	V3
Approved by	Board of Trustees
Review	Biannually
Approval Date	July 2026

Inclusion – Improving education for everyone.

Integrity – We are consistently open, honest, ethical, and genuine.

Initiative – We have the courage to always seek a better way to a better future.

Inspiration – We use our drive and commitment to energise, engage and inspire.

Involvement –We encourage our community to take ownership and responsibility.

Table of version reference

Revision	Date	Comments
V2	11/04/24	Format Changes on various pages. Pg 5 inclusion of trust code of conduct Pg 6 & Pg12 highlighted storage stick forbidden, reference added to the Equality act and protected characteristics Pg 7 wording changes to INMAT email address Pag 8 added list of cloud based suppliers Pg 9 added social accounts managed by Comms lead or Head Teacher Pg 10 added further polices Pg 12 added Phishing and Cyber Training Pg 13 Updated Internet access section Pg 13 added further information on Cyber awareness and response plans
V3	07/07/2026	Pg 6 Additions to Unacceptable Use section Pg 13 Replace Webroot with Opentext EDR Pg 15 Add AI Policy to related policies Pg 19 Clauses added to Older Pupil User Agreement Pg 20 Clauses added to Younger Pupil User Agreement Pg 21 Clause added ref trust approved AI tools to Staff/Governors User Agreement Appendix 2, 3 & 4 all now appendix 2 Renamed remaining appendices

Contents

1. Introduction and Aims

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

However, the ICT resources and facilities our trust uses 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 employees, pupils, parents, trustees and governors
- Establish clear expectations for the way all members of the trust community engage with each other online
- Support the trust's policy on data protection, online safety and safeguarding
- Prevent disruption to the trust through the misuse, or attempted misuse, of ICT systems
- Support the trust in teaching pupils safe and effective internet and ICT use
- This policy covers all users of our trust's ICT facilities, including governors, Employees, pupils, volunteers, contractors, and visitors.
- Breaches of this policy may be dealt with under the INMAT Code of Conduct.

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 2024
- 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 to use the ICT facilities, including governors, Employees, 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 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 appendix 6 for a glossary of cyber security terminology.

4. Unacceptable Use

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

Unacceptable use of the trust's ICT facilities includes:

- Using the trust's ICT facilities to breach intellectual property rights or copyright
- Using the trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust's code of conduct, 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 trust, or risks bringing the trust into disrepute
- Sharing confidential information about the trust, its pupils, or other members of the trust community
- Connecting any device to the trust's ICT network without approval from authorised personnel
- Setting up any software, applications, or web services on the 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
- Inputting sensitive Trust data or Pupil IP into unapproved AI tools
- Using AI to bypass network filters or create deceptive content (eg. deepfakes)
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the 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 trust
- Using websites or mechanisms to bypass the trust's filtering mechanisms
- Engaging in content or conduct that is in breach of the Equality Act 2010, discriminatory to protected characteristics, is radicalised, extremist, racist, anti-Semitic, or discriminatory in any other way
- Leaving ICT equipment anywhere other than on your person, at work or at home e.g. in the car
- Using a (generic portable solid-state data storage device): data stick, pen drive, thumb drive, USB drive is strictly forbidden
- This is not an exhaustive list. The trust reserves the right to amend this list at any time. The headteacher, LAC and Trust will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the trust's ICT facilities

4.1 Exceptions from unacceptable use

Where the use of trust ICT facilities (on the trust premises 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 headteacher's discretion.

Employees will seek advice and if needed permission from the headteacher should technology need to be used in other circumstances e.g.: on residentials and day visits.

4.2 Sanctions

Pupils and Employees who engage in any of the unacceptable activity listed above may face disciplinary action in line with the trust's policies on behaviour and Code of Conduct. This could include referrals to the LADO and result in warnings and dismissal.

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

5.1 Access to trust ICT facilities and materials

The trust's IT provider manages access to the trust's ICT facilities and materials for trust Employees.

That includes, but is not limited to:

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

Employees will be provided with unique log-in/account information and passwords that they must use when accessing the trust's ICT facilities.
Employees 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 owner e.g.: Line manager

5.2 Use of emails

The trust provides each employee with an INMAT email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the trust has provided. Employees must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Employees 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.

Employees 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 Employees 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 Employees send an email in error that contains the personal information of another person, they must inform the headteacher/line manager immediately and follow our data breach procedure.

5.3 Use of phones

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

Trust phones must not be used for personal matters.

Employees 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.

5.4 Personal use

Employees are permitted to occasionally use 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/line manager 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 teaching 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 Employees or pupils from using the facilities for work or educational purposes
- Employees may not use the trust's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos)
- Employees should be aware that use of the trust's ICT facilities for personal use may put personal communications within the scope of the trust's ICT monitoring activities (see section 5.5)
- Where breaches of this policy are found, disciplinary action may be taken
- Employees should be aware that personal use of ICT (even when not using trust ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them
- Employees should take care to follow the trust's guidelines on social media (see appendix 1) and use of email (see section 5.2) to protect themselves online and avoid compromising their professional integrity

5.5 Personal social media accounts

Employees should follow the INMAT Employees code of conduct and ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The trust has guidelines for Employees on appropriate security settings for social media accounts (see appendix 1).

5.6 Remote access

We allow Employees to access the trust's resources remotely inc : O365, Arbor, PSF, IMP, My Concern and Educational support and planning programmes for areas such as Maths, English and PE.

Employees accessing the trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Employees must be particularly vigilant if they use the trust's ICT facilities outside the trust and take such precautions as they may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information that 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.

5.7 Trust social media accounts

INMAT and its Schools have an official Facebook / X and Instagram page, managed by the headteacher and Central Comms. Named Employees can also access and post online with guidance given from the

headteacher /Central Comms. Employees who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

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

5.8 Monitoring of trust network and use of ICT facilities

The 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 Employees may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law

The trust monitors ICT use in order to:

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

Filtering and monitoring, compliant with the requirements of Keeping Children Safe in Education 2024 DfE Statutory guidance is in operation within the Trust. The reports generated as a result of filtering and monitoring activities are only accessible to authorised users.

6. Pupils

6.1 Access to ICT facilities

Laptops and tablets are available to pupils only under the supervision of Employees

Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of employees.
Pupils will be provided with a TEAMs account linked to the trust's virtual learning environment, which they can access from any device.

6.2 Search and deletion

Under the Education Act 2022, and in line with the Department for Education's guidance on searching, screening and confiscation, the trust has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under trust rules or legislation.

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

Employees 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 the trust

The trust will sanction pupils, in line with the Expectation (Behaviour) policy, Anti-bullying policy and safeguarding policy if a pupil engages in any of the following **at any time** (even if they are not on trust 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'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 trust, or risks bringing the trust into disrepute
- Sharing confidential information about the trust, other pupils, or other members of the trust 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'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 trust's ICT facilities as a matter of course.

However, parents working for, or with the 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 trust'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 Employees.

7.2 Communicating with or about the trust 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 through our website and social media channels.
We ask parents to sign the agreement in appendix 2.

8. Data security

The trust 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 trust cannot guarantee security. Employees, pupils, parents and others who use the trust's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the trust'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 Employees 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'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's ICT facilities.

Any personal devices using the 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 trust's data protection policy as outlined by INMAT

8.4 Access to facilities and materials

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

These access rights are managed by the headteacher/central office and IT support.

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 immediately.

Users should always close windows, 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 or when moving working location.

8.5 Encryption

The trust ensures that its devices and systems have an appropriate level of encryption.
Trust employees can only store trust related work using TEAMs and their one drive. Memory sticks/external hard drives are **not permitted** to be used.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The trust will:

- Work with employees, trustees, governors and trust IT support to make sure cyber security is given the time and resources it needs to make the trust secure
- Provide regular updates for employees and timely reminders regarding password protection.
- Make sure employees, trustees, governors are aware of its procedures for reporting and responding to cyber security incidents
- Monitor IT software needs regularly checking for updates or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Ensure that there is a complete backup of systems and data, which is stored offsite and providing at least 30 days of snapshots to ensure recovery from ransomware attacks
- Phishing test termly
- Annual Cyber Security training

Put controls in place that are:

Proportionate: the trust will verify this using a third-party audit set by INMAT 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 trust 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

Make sure Employees:

- Use TEAMs to access information off site
- Enable multi-factor authentication where they can, on things like trust email accounts
- Store passwords securely using a password manager
- Make sure ICT Employees conduct regular access reviews to make sure each user in the trust has the right level of permissions and admin rights
- Have a virtual hosted firewall in place
- 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
- Work with our Trust to see what it can offer the trust regarding cyber security, such as advice on which service providers to use or assistance with procurement
- The trust wireless internet connection is secured
- Make sure all schools have a cyber incident response plan, 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.

10. Internet access

INMAT uses Opentext EDR which has a browser extension that provides browser protection. The web filtering solution is with Securly at all of our schools regardless of ISP.

10.1 Pupils

Pupils access the trust's Wi-Fi when using trust devices. Pupils access these using a their own log in alongside their own accounts for TEAMs and other trust subscribed programs. The Wi-Fi password is set on student devices through server policy, so the wireless key is never known to students. In certain specific circumstances such as to support pupils with SEND, specific authorisation maybe given to access Wi-Fi through pupil's own devices.

10.2 Parents and visitors

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

The headteacher will only grant authorisation if:

- Parents are working with the trust in an official capacity (e.g., as a volunteer or as a member of the PTA)
- Visitors need to access the trust'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)
- Employees must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. General network security

INMAT will ensure that the schools networks connections are secure.

Where possible, schools will have a guest wireless to provide network isolation and prevent the Employees wireless key and network from becoming compromised.

12. Monitoring and review

The headteacher and IT support team monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the trust.

This policy will be reviewed every 2 years.

12. Related policies

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

- Safeguarding and child protection
- Behaviour
- Employees Code of Conduct
- Anti-Bullying Policy
- AI Policy

APPENDIX 1: **FACEBOOK CHEAT SHEET FOR EMPLOYEES**

Don't accept friend requests from pupils on social media

10 rules for trust Employees on Social Media

- Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
- Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
- Check your privacy settings regularly
- Be careful about tagging other Employees members in images or posts
- Don't share anything publicly that you wouldn't be just as happy showing your pupils
- Don't use social media sites during trust hours
- Don't make comments about your job, your colleagues, our trust or your pupils online – once it's out there, it's out there
- Don't associate yourself with the trust on your profile (e.g., by setting it as your workplace, or by 'checking in' at a trust event)
- 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
- 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 to do 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
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 Employees 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 Employees 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/CARERS AND PUPILS

Name of parent/carer:

Name of child:

AGREEMENT FOR PARENTS AND CARERS

Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels:
Our official Facebook and Instagram pages
Email/text groups for parents (for school announcements and information)
Our virtual learning platform
Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
When communicating with the school via official communication channels, or using private/independent channels to talk about the trust, I will:

- Be respectful towards members of Employees, 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 schools Facebook page, or personal social media to complain about or criticise members of Employees. This is not constructive, and the trust can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the schools 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 Employees 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

AGREEMENT FOR PUPILS (KS2)

When using the schools' 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 Employees 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 will not use AI to complete my homework and present it as my own.
- I will not enter personal information into AI chatbots.
- I will not use AI to generate fake images or messages.
- 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.

AGREEMENT FOR YOUNGER PUPILS (Foundation/KS1)

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
- 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 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 will not use AI to complete my homework and present it as my own.
- I will not enter personal information into AI chatbots.
- I will not use AI to generate fake images or messages.
- 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.

Please sign to say you have read and understood the above:

Parent/Carer Signature: _____

Pupil Signature: _____

APPENDIX 3: ACCEPTABLE USE AGREEMENT FOR EMPLOYEES, GOVERNORS VOLUNTEERS AND VISITORS

Name of Employee, Governor. Volunteer, Visitor:

When using the trust's ICT facilities and accessing the internet in trust, or outside trust 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'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's network
- Share my password with others or log in to the trust's network using someone else's details
- Share confidential information about the trust, its pupils or Employees, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the trust
- I understand that the trust will monitor the websites I visit and my use of the trust's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside trust, and keep all data securely stored in accordance with this policy and the trust's data protection policy.
- I will only use Trust approved AI tools and will never input personal, safeguarding or commercially sensitive data into unapproved public models.
- 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's ICT systems and internet responsibly and ensure that pupils in my care do so too

Signature: _____

APPENDIX 4: GLOSSARY OF CYBER SECURITY TERMINOLOGY

These key terms will help you to understand the common forms of cyber-attack and the measures the trust will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

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

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

APPENDIX 4: Device Receipt

Device Receipt

I confirm that I have received the below device(s) and I have read and agreed to the INMAT ICT acceptable use policy.

Device description
Model
Serial number

Name _____

Sign _____

Date _____