IT and Internet Acceptable Use Policy

Approved by:	Board of Trustees	**Date:**	September 2025
Date Created	October 2023		
Last reviewed on:	September 2025		
Next review due by:	Autumn 2026		

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way Inspire Multi Academy Trust (MAT) and our schools work, and is a critical resource for pupils, staff (including the senior leadership team), members, trustees, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of our schools.

However, the ICT resources and facilities we use across Inspire MAT could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

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

Breaches of this policy by pupils may be dealt with under our Behaviour and Discipline Policy for pupils and for staff under our Disciplinary Policy and Staff Behaviour Policy.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** 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 ICT device system or service that may become available in the future which is provided as part of the Trust's ICT service

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

Please 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. 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 ICT facilities to breach intellectual property rights or copyright
- Using the ICT facilities 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
- 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
- Activity which defames or disparages the Trust or an individual school, or risks bringing the Trust or individual school into disrepute
- Sharing confidential information about the Trust or an individual school, its pupils, or other members of the Trust or school 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 programme, tool or item of software designed to interfere with the functioning of the Trust's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to the Trust's ICT facilities
- Removing, deleting or disposing of the Trust's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel 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 or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Engaging in any illegal activities

This is not an exhaustive list. The Trust reserves the right to amend this list at any time.

The Chief Executive Headteacher and Academy Headteachers will use their 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 the ICT facilities (on the Trust/school 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 Chief Executive Headteacher's or Academy Headteacher's discretion.

Such requests should be submitted to the school Headteacher (for school-based employees or pupils) or Chief Executive Headteacher (for central team employees) in writing. The request will be duly considered and a decision will be communicated to the individual.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action. Action against pupils may be dealt with under our Behaviour and Discipline Policy and for staff under our Disciplinary Policy or Staff Behaviour Policy.

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

5.1 Access to school ICT facilities and materials

The Trust's external IT provider manages access to the ICT facilities and materials for pupils, members, trustees, governors and school staff. That includes, but is not limited to:

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

Members, trustees, governors and staff will be provided with unique login/account information and passwords that they must use when accessing the Trust's ICT facilities.

Users who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the external IT provider.

5.1.1 Use of phones and email

The Trust provides each member, trustee, governor and member of staff with an Office 365 account and email address for work related use.

This email account should be used for work purposes only. Users should enable multi-factor authentication on their account via the Cisco Duo application, when accessing ICT services off-site. This will prevent unauthorised users accessing our network.

All work-related business should be conducted using the email address we have provided. Users must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Users 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.

Users must take extra care when sending sensitive or confidential information by email. Any emails or attachments containing sensitive or confidential information, sent to external recipients should be encrypted via Cisco Secure Email so that the information is only accessible by the intended recipient.

If users 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 to any other party.

If a user sends an email in error that contains the personal information of another person, they must inform the Trust's Data Protection Officer immediately and follow our data breach procedure. In this instance, users should contact the recipient without delay and seek the deletion of the email and all attachments, including deletion from deleted items.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use landline or mobile phones provided by the Trust to conduct all work-related business.

Trust/school landline and mobile phones must not be used for personal matters, other than in exceptional circumstances, with permission from the Chief Executive Headteacher, Headteacher or member of the senior leadership team.

Staff who are provided with Trust mobile phones as equipment to support their role must abide by the same rules for ICT acceptable use as set out in section 4.

The Trust can utilise call recording software to record incoming and outgoing phone conversations as required. Where this is the case, the caller must be made aware if they are to be recorded.

Staff who would like to record a phone conversation should speak to the Data Protection Officer. All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.2 Personal use

Staff are permitted to use Trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Chief Executive Headteacher may instruct the external IT provider to withdraw or restrict this permission at any time and at their discretion. In such cases, staff will be informed.

Personal use is permitted provided that such use:

- Does not take place during pupil contact time, teaching time or pupil facing time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Takes place during staff break or non-pupil facing time
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Users may not use the ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Users should be aware that use of the 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, in line with agreed policies.

All users, particularly 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/carers could see them.

Members, trustees, governors and staff should take care to follow the Trust's guidelines on use of 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, trustees, governors and staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. The Trust has guidelines for appropriate security settings and general guidance for social media accounts (see appendix 1).

5.3 Remote access

We allow staff to access the Trust's ICT facilities and materials remotely, on Trust devices. They should dial in using Cisco Connect, a virtual private network (VPN) which can be set up on our devices by the external IT provider.

Staff accessing the Trust'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 ICT facilities outside school and must take such precautions as required 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

Each Inspire academy have an official school Facebook account, managed by the Headteacher and designated staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access it.

Each school has guidelines for what should or should not be posted on its social media accounts. Those who are authorised to manage, or post to the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Trust reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Web searches on any browser used
- Bandwidth usage
- Email accounts including items sent, received or filed in an email folder
- Telephone calls sent and received (landline and mobile)
- User activity/access logs
- Any other electronic communications

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

Internet searches and internet activity are monitored using the Securly platform. Our central team receive alerts showing all web searches and internet activity for all registered users, as well as alerts where Securly has blocked traffic/content deemed inappropriate.

The school monitors ICT use in order to:

- Obtain information related to Trust business

- Investigate compliance with Trust 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

Our Board of Trustees is responsible for making sure that the Trust meets the DfE's filtering and monitoring standards and appropriate filtering and monitoring systems are in place. Users are aware of those systems and trained in their related roles and responsibilities.

The Securly platform issues an alert to the central services team, whenever a user tries to access a blocked site, or search for a blocked term. Securly determines which sites and searches are blocked by means of a blacklist, with a whitelist allowing us to allow access, if a site is wrongly categorized and blocked.

The central services team conduct an initial review of alerts, to determine whether a user has contravened the acceptable use policy. Where the policy has been contravened, this matter should be referred to the Headteacher (or Deputy in their absence) or Chief Executive Headteacher, to consider disciplinary action, in line with agreed policies.

Our external IT provider regularly review the effectiveness of the Trust's monitoring and filtering systems.

Our schools have a designated safeguarding lead (DSL) who will take lead responsibility for understanding the filtering and monitoring systems and processes in place. They will be supported by the external IT provider and our central services team.

Where appropriate, staff may raise concerns about monitored activity with their school's DSL and the Business Relationships and Governance Manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

The following ICT equipment is available for pupil use:

- Computers and equipment in the school's ICT suite (desktop and laptop PCs and tablet devices) are available to pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Pupils will be provided with an account for any online intervention programmes, for example Reading Plus, which they can access from any device connected to the internet.

6.2 Search and deletion

Pupils are not permitted to bring a personal mobile phone into school. If a pupil brings a mobile phone onto site, this is handed in to the school office for safe-keeping and returned to the pupil at the end of the school day.

Under the Education Act 2011, our Headteachers, and any member of staff authorised to do so by the Headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out, **and/or**
- Is evidence in relation to a criminal offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from The Headteacher, Designated Safeguarding Lead or a Deputy Designated Safeguarding Lead
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the Behaviour Policy
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit a criminal offence

If inappropriate material is found on the device, it is up to the Headteacher/DSL or their nominated Deputy to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable.

If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Not copy, print, share, store or save the image

- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour Policy which is reviewed annually, at the start of each academic year

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the Complaints Policy.

6.3 Unacceptable use of ICT and the internet outside of school

Our schools will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises when using school equipment, programmes etc.):

- 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 making 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 or 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 the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

Across our Trust, parents/carers do not have access to our ICT facilities as a matter of course.

However, parents/carers working for, or with, the Trust or an individual 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 Chief Executive Headteacher or Academy Headteacher discretion.

Where parents/carers are granted access in this way, they must abide by this policy in the same was 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/carers 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/carers to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about pupil activity

Our schools will make parents and carers aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data Security

The Board of Trustees are responsible for making sure we have the appropriate level of security protection and procedures in place to safeguard ICT systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber-crime technologies.

Staff, pupils, parents/carers and others who use the Trust's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Passwords must be suitably complex and robust, they should not contain any words which are part of your username, be at least 6 characters long and fill at least 3 of the 4 follow criteria:

- at least 1 Capital Letter
- at least 1 Lower Case letter
- at least 1 Number
- at least 1 Special Character (e.g.: !"£$%^&*()@~?>

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, visitors or volunteers who disclose account or password information may have their access rights revoked.

Account passwords are set to automatically expire after 30-days.

The external IT support team will generate passwords for pupils using the required password manager or 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 Trust's ICT devices that support software updates, security updates and anti-virus products will have these installed, and 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 Trust Data Protection policy.

8.4 Access to facilities and materials

All users of the Trust's ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by the external IT provider.

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 external IT provider and their Line Manager 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 shut down completely at the end of each working day.

8.5 Encryption

The Trust makes sure that its devices and systems have an appropriate level of encryption.

Our Central Services staff and school staff may use personal devices (including computers, laptops, tablets etc.) to access Trust/school data, work remotely however, personal data (such as pupil information) should not be taken out of school on personal devices unless they have been specifically authorised to do so by the Chief Executive Headteacher or academy Headteacher.

Use of such personal devices will only be authorised in exceptional circumstances and if the devices have appropriate levels of Security and encryption, as defined by the external IT provider.

Wherever possible, USB drives and flash drives should not be used and staff should instead use the secure cloud storage facility provided for them and linked to their work Office 365 account (currently OneDrive).

9. Protection from cyber attacks

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

The Trust and our schools will:

- Work with members, trustees, governors, staff and the IT provider to make sure cyber security is given the time and resources it needs to make our systems secure
- Provide training for staff (within induction for new starters) 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 objectively test that what it has in place is effective
    - Multi-layered: everyone will be clear on what to look out for to keep our systems safe
    - Up to date: with a system in place to monitor when we need to update our software
    - Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be
- Back up critical data daily and store these backups on premise as well as in the Cloud off-site
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to ESS, our cloud-based provider.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure the external IT provider 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 checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the external IT provider including, for example, how the Trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our LA and/or the external IT provider to see what it can offer the Trust/schools regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The Trust's wireless internet connection is secure. We use Cisco Meraki and MERU wireless devices across the Trust estate, with a package of Cisco products complimenting this, such as Cisco Umbrella.

We use web-filtering from Securly to monitor all break-out to the internet.

Securly provides web filtering, to block searches for restricted content and block sites. A Blacklist and Whitelist approach allows the external IT provider to add or allow sites, as required.

We have a separate SSID for staff, visitors and pupils with appropriate restrictions set for each group. Securly monitors and protects all traffic.

10.1 Pupils

Web-filtering controls and restrictions on pupil accounts are in place, to prevent them accessing inappropriate content. If a new site appears which staff feel in not appropriate for pupils, the external IT provider can restrict access via the Blacklist, or enable access where an item is wrongly categorised to the Whitelist.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's Wi-Fi unless authorisation is granted by the Chief Executive Headteacher, Headteacher or senior leader.

Authorisation will only be granted if:

- Parents/carers 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 being taken.

11. Monitoring and review

The Board of Trustees, supported by the external IT provider, the Central Services team and Headteachers 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 annually and will be presented to the Board of Trustees for approval.

12. Related policies

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

- Behaviour and Discipline
- Code of Conduct for Parents, Carers and Visitors
- Data Protection
- Disciplinary
- Mobile phone usage
- Online Bullying
- Online Safety
- Photography and Digital Imagery
- Preventing Extremism and Radicalisation
- Safeguarding/Child Protection
- Staff Behaviour

Appendix 1:

Facebook Cheat Sheet

This document is intended to provide general advice to members, trustees, governors and staff who use social media platforms outside of their work role.

Do not accept friend requests from pupils on social media

10 tips to consider

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 you don't, make sure 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 happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our 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 social media apps from your mobile phone. The apps recognise Wi-Fi connections and makes friend/follow suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

1. 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
2. Don't forget to check your **old posts and photos**
3. 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
4. **Google your name** to see what information about you is visible to the public
5. Prevent search engines from indexing your profile so that people can't **search for you by name**
6. Remember that on some platforms **some information is always public**: for example, 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

1. In the first instance, ignore and delete the request. Block the pupil from viewing your profile
2. Check your privacy settings again, and consider changing your display name or profile picture
3. 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/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
4. Notify the Headteacher or SLT member about what's happening

A parent/carer adds you on social media

1. It is at your discretion whether to respond. Bear in mind that:

- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school

2. Pupils may then have indirect access through their parent/carer'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/carer know that you're doing so

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

1. **Do not** retaliate or respond in any way
2. Save evidence of any abuse by taking screenshots and recording the time and date it occurred
3. Report the material to the social media platform (e.g. Facebook, Instagram etc.) and ask them to remove it
4. If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
5. If the perpetrator is a parent/carer 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
6. 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

This form is intended for use with parents/carers who are working with the Trust or one of our schools in an official capacity (e.g. as a volunteer or as a member of the PTA).

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, Inspire Multi Academy Trust and our family of academies. Our schools use the following channels to communicate: • Our official social media pages • Email/text groups for parents (for school announcements and information) • Our communication apps • Our virtual learning platforms 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). These channels are not within the control of Inspire MAT our academies.	
When communicating with the us via official communication channels, or using private/independent channels to talk about the Trust/school, I will: • Be respectful towards members of staff, and the 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 Facebook 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 unless they are 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 the other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

This form is intended for use with Key Stage 2 pupils.

Acceptable use of ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the Trust/school ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher or member of school staff being present, or without permission from a teacher or member of school staff • Use them to break school rules • Access any inappropriate websites • Access social networking sites (unless my teacher or a member of school staff 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 or member of school staff • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video • Share my password with others or log in to the network using someone else's details • Bully other people • Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work I understand that the Trust/school will monitor the websites I visit and my use of the 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 ICT systems and internet responsibly. I understand that the school can discipline me if I carry out unacceptable actions 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 Trust/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 Trust/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

This form is intended for use with Key Stage 1 pupils.

<table>
<tr><th colspan="2">Acceptable use of the school's ICT facilities and internet:
agreement for pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not:
Use them without asking a teacher or staff member first, or without a teacher or staff member 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 or staff member 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
Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work
I understand that the Trust/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 carry out unacceptable actions online, even if I'm not in school when I do them.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the Trust/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 Trust/school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 5: Acceptable use agreement for staff, members, trustees, 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/member/trustee/governor/volunteer/visitor:	
When using the Trust/school 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 Trust/school's reputation • Access social networking sites or chat rooms for personal use • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the Trust/school network • Share my password with others or log in to the Trust/school network using someone else's details • Share confidential information about the Trust/school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the Trust/school	
I understand that the Trust/school will monitor the websites I visit and my use of the 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 Trust's Data Protection Policy. I will let the designated safeguarding lead (DSL) and the external IT provider know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the Trust/school ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/member/ trustee/ governor/ volunteer/visitor):	**Date:**

Appendix 6: Glossary of cyber Security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the Trust and our academies will put in place.

They are from the National Cyber Security Centre (NCSC) glossary.

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

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as 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	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix 7: Display Screen Equipment (DSE) Guidance

Please refer to the guidance below when you are using your computer/laptop in connection with Trust business. Users have a duty of care to themselves to observe good practice in the use of DSE work.

If you require any advice or support or specialist equipment please contact your School Business Manager.

Seating - general guidelines

Chair design

All seating provided for work should:

- Support you in a position which allows work to be done comfortably.
- Allow you to change position easily.
- Not compress the thighs and buttocks.
- Suit any special needs you may have.
- Be matched to the dimensions and layout of your workstation.

The seat must be:

- Adjustable in height (without the use of tools) to accommodate you whether you are very short or very tall.
- Wide enough for big people and deep enough to support the legs of tall people.
- Covered in a porous material as well as being well padded.

The backrest

The height should be adjustable (unless giving complete support to the back). It should give firm support to the lower and middle parts of the back. A tiltable backrest prevents your body from having to lift, slide or twist to make backward and sideways movements.

Armrests

Armrests are not essential, but can provide extra comfort, say during natural pauses. The height of armrests is important: they must not prevent you from drawing close to your desk and they must give support without you having to slouch. Height adjustable armrests are preferable.

Moveability

Your chair should have a minimum of 5 castors or glides. This makes moving it backwards and forwards or from side to side much easier and places less stress on your body. Care needs to be taken that the chair doesn't slide away too easily when you sit or stand up.

Footrests

If your feet are a little short of the floor, after you have adjusted your chair to suit the height of the work you are doing, a footrest will help. And if you ask, one will be provided.

Your environment and workstation

What do you need?

1 Good general lighting to cover all the work done. It should not be too bright and avoid reflections as these conditions lead to fatigue and stress. Anti-glare screens should be a last resort.

2 Use local lighting to illuminate documents if required. Adjust so as not to annoy your neighbours.

3 Noise emitted by equipment, especially other peoples', can be a real nuisance and should be eliminated where possible.

4 There should be sufficient legroom to enable you to get in and out easily.

5 If there are variations in natural light, the use of window coverings may help to even them out.

6 Software should be appropriate for the task and easy to use.

7 The monitor needs to be adjustable for rotation and pitch (making it easier to read from). The screen should provide a stable image, be adjustable for brightness and contrast and be glare and reflection free.

8 The keyboard should be comfortable to use, non-reflective and with characters that are easy to read.

9 Your desk should be big enough to hold the equipment and with enough space to allow for documents and any other work you may want to do.

10 The primary requirement for a work chair is that it is adjustable, allowing you to achieve a comfortable position.

11 Footrests may be necessary when, having adjusted everything else, you are unable to rest your feet flat on the floor.

Mouse - Using a mouse, trackerball or any other pointing device for prolonged periods can cause problems. Make use of any opportunities for breaking up the work or using keyboard shortcuts.