

IncludEd Learning

Independent Specialist Education Provider



ICT AND INTERNET ACCEPTABLE USE POLICY

Contents

1. Introduction and Aims	3
2. Relevant Legislation and Guidance.....	3
3. Definitions	4
4. Unacceptable Use.....	4
5. Staff including Advisory Panel, Volunteers, and Contractors).....	6
6. Students.....	9
7. Parents/Carers	12
8. Data Security.....	13
9. Protection from Cyber Attacks	15
10. Internet Access	16
11. Monitoring and Review.....	17
12. Related Policies	17
Appendix 1: Social Media Cheat Sheet for Staff.....	18
Appendix 2: - Acceptable Use of the Internet: Agreement for Pupils.....	20
Appendix 3: Acceptable Use Agreement for Staff.....	21
Appendix 4: Glossary of cyber security terminology	23

→ 1. Introduction and Aims

Information and communications technology (ICT) is an integral part of the way IncludEd Learning works, and is a critical resource for students, staff (including the senior leadership team), advisor panel, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

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

This policy aims to:

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

This policy covers all users of the schools ICT facilities, including the advisory panel, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy and staff 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 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 2026](#)
- [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 device system or service that may become available in the future which is provided as part of the school's ICT service.
- **Users:** anyone authorised by the school to use one of the school's ICT facilities, including the advisory panel, staff, students, 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 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.

See appendix 6 for a glossary of cyber security terminology.

→ 4. Unacceptable Use

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

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity ☐ Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams

•

- Activity which defames or disparages the school, or risks bringing one of the school's schools or services into disrepute
- Sharing confidential information about the school, its students, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school'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 school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school'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 school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Unacceptable use of artificial intelligence (AI) tools: any tasks linked to the sharing of personal data. Personal data such as full names, addresses and dates of birth must not be inputted into AI tools under any circumstance

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Head of School or any other relevant member of the senior leadership team will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on 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 Head of School's discretion.

- staff may use AI tools and generative chatbots for lesson planning, document presentation
- assisting with the wording of information for administrative tasks and learning resources

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI, for example in IT lessons or AI-generated images. All AI-generated content must be properly attributed
- If staff choose to use AI tools, they are responsible for checking the output generated. This could include proof reading for spelling and grammar errors and fact checking. Staff should also be aware that children may use AI at home and to educate them on the potential risks and challenges.

4.2 Sanctions

Children and young people and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies.

All policies can be found on the school's website: www.includedlearning.co.uk

→ 5. Staff Including Advisory Panel, Volunteers, and Contractors) Accessibility Features

To ensure an inclusive and supportive work environment, our accessible use of ICT policy mandates that all staff, including those with deafness or vision impairment, have access to agreed-upon accessibility features. This includes providing assistive technologies such as screen readers, magnification tools, audio description AI and captioning services. We are committed to regularly reviewing and updating these features in consultation with our staff to ensure they meet individual needs and enhance productivity. By prioritising accessibility, we aim to empower all employees to perform their roles effectively and contribute to our organisation's success.

5.1 Access to school ICT facilities and materials

The school IT manager manages access to the school's ICT facilities and materials for school and service staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff 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 Head of School.

5.2 Use of phones and email

IncludEd Learning provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s). All work-related business should be conducted using the email address the school has provided.

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

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Head of School and IT provider immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or students. Staff must use phones provided by the school to conduct all work-related business. If an emergency situation (such as accompanying a student to hospital) needs numbers to be released a member of SLT should be informed

School phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

5.3 Personal use

Staff are permitted to occasionally use school/ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Head of School may withdraw or restrict this permission at any time and 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 staff or students from using the facilities for work or educational purposes

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

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff 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 students and parents/carers could see them.

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

5.4 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Personal social media accounts should be saved as private use and not public.

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

5.5 Remote access

We allow staff to access the school's ICT facilities and materials remotely by using the shared drive on googledrive.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside school or work and must take such precautions as Atlas may require 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 available on the staff hard drive.

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

To safeguard and promote the welfare of students and provide them with a safe environment to learn, the school 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
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

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

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Our Advisory Panel is responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place
- For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's Designated Safeguarding Lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

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

→ 6. Students

6.1 Access to ICT facilities

Computers and equipment in the school ICT suites are available to students 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.

6.2 Search and deletion

Under the Education Act 2011, the Head of School, and any member of staff authorised to do so by them, can search students 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 students, **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 an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of students
- 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 students and staff. If the search is not urgent, they will seek advice from senior leaders
- Explain to the students 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 students's and parents/carers co-operation

The authorised staff member should:

- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk
- Contact the parents/carers

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 an offence

If inappropriate material is found on the device, it is up to the Head of School 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 student (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 school 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 students 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](#)

Any complaints about searching for, or deleting, inappropriate images or files on students's devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, if any engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or 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 it into disrepute
- Sharing confidential information about the school, other students, 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

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

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the advisory panel may be granted an appropriate level of access, or be permitted to use the ICT facilities at the head of schools discretion.

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

7.2 Communicating with or about the school or one of its schools/services online

We believe it is important to model for students, 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 students, especially when communicating with one of the schools 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 students activity

Each school will ensure that parents and carers are made aware of any online activity that their students are being asked to carry out.

When we ask students 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 students will be interacting with online, including the purpose of the interaction.

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

→ 8. Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its 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 school'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 school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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

Members of staff or students who disclose account or password information may face disciplinary action.

Staff should not share the log in details with other staff members.

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

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

Passwords will be updated where deemed necessary.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will 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 school's [data protection policy](#).

Data Protection Policy

8.4 Access to facilities and materials

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

These access rights are managed by the head of school.

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 Head of School 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 school makes sure that its devices and systems have an appropriate level of encryption.

All removable media must be authorised and offer data security options like encryption to safeguard data. Staff should not use USB storage devices for school work and data storage. The school offers remote access which connects to the school's network, this is the solution to remove the need for USB storage, the remote access system and cloud system Microsoft's Office 365 are also available to help transfer data securely. Removable media includes but is not restricted to:

- CDs / DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks - NOT TO BE USED AT ALL
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- MP3 Players
- Digital Cameras
- Bluetooth device
- Webcams
- Backup tapes or drives
- Personal cloud storage platforms

→ 9. Protection from Cyber Attacks

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

- Work with the advisory panel to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff 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 school will verify this using a third-party audit to 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 the school needs to update its software
- **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Back up critical data least once a day and store these backups on cloud based backup systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS)

Make sure staff:

- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the [Cyber Essentials](#) certification

- Develop, review and test an incident response plan with the IT department including, for example, how the school 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 after a significant event has occurred, using the NCSC's ['Exercise in a Box'](#)
- Work with partners to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

→ 10. Internet Access

The school's wireless internet connection is secure.

To monitor all internet usage and are able to perform regular checks on the system.

- Filtering is monitored by using Smoothwall
- Smoothwall will provide the school with up to date real time information if there are any breaches

There is wifi log in for:

- Staff
- Guests

10.1 students

students can only access the school WiFi through school issued devices.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school school will not be permitted to use the school's WiFi unless specific authorisation is granted by the head of school.

The head of school will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the advisory panel)
- Visitors need to access the school's WiFi 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 WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

→ 11. Monitoring and Review

The school leadership team will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The head of school and the advisory panel is responsible for reviewing this policy.

→ 12. Related Policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Data protection
- Mobile phone and devices policy
- AI policy

→ Appendix 1: Social Media Cheat Sheet for Staff

10 Rules for school staff on social media sites

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 school students
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, the school or school/service or your students online – once it's out there, it's out there
8. Don't associate yourself with the school or school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or students)

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 student adds you on social media

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

A parent/carer adds you on social media

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
- 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

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the social media site or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- 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
- 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 Internet Use - Pupils

This document is a guide to pupils to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password.
- I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or alter computer settings.
- I will hand in personal use my personal hand held devices (e.g. mobile phone/ipad) in school at times that are permitted. This is commuting to and from school, or to contact parents after participation in an extra- curricular activity. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them. For my own safety and that of others, I will not disclose personal information about myself or others when on-line.
- I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. Where the material I research on the Internet is protected by copyright,
- I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

StudentName:	
Signed Student:	
Signed Parent/Carer:	Date:

→ Appendix 3: Acceptable Internet Use - Staff

Responsible Use Agreement

I understand that I must use ICT systems in a responsible way ensuring no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the use of ICT for enhancing learning and will ensure all learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students.

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, website) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person (see policy charts).

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I will not use my personal equipment to record these images. I will not use chat and social networking sites in the school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

IncludEd Learning, partner schools and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (Ipads/laptops/mobile phones/USB devices etc) in the school, I will follow the rules set out in this agreement, in the same way as if I was using the school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems. I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not (unless I have permission) make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Sharing Information Policy. Where personal data is transferred outside the secure LA network, it must be encrypted.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school and my use of personal equipment in the school or in situations related to my employment by IncludEd Learning.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, suspension, referral to the Advisory Panel or the Local Authority and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use IncludEd's Learning ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer/Advisory Board Member

Name:	
Signed:	
Date:	

→ 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 school 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.
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.