CUMBRIA FUTURES
FEDERATION

Policy Reference H05

ICT and Internet Acceptable Use Policy

Every school within Cumbria Futures Federation aims to provide a safe and hardworking environment where every child can be successful, whatever their abilities.

Our Values

- Courage and Compassion
- Inclusion and Equality
- Respect and Courtesy
- Optimism and Perseverance
- Forgiveness and Tolerance
- Ambition and Achievement

Version No	Author/Owner	Date Written	Note of amendments made
2022-01	JR/JG	November 2022	New Policy from model policy

Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for students, staff (including senior leadership teams), governors, volunteers and visitors.

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

This policy aims to:

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

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

Breaches of this policy may be dealt with under our disciplinary and behaviour policies.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, students, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 5 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see 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 (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school or any member of its community, or risks bringing the school or a member of its community 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 program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school’s ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school’s filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or the IT/Network Manager will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school’s ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the 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 Headteacher's discretion. Permission must be explicitly sought from the Headteacher in writing and in advance of such activities.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on discipline and behaviour. Copies of policies can be found on the school's website and/or internal systems

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

5.1 Access to school ICT facilities and materials

The school's IT/Network Manager, under the direction of the Director of Finance and Operations manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

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

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT/Network Manager. Requests for updated permissions should be made in writing.

5.1.1 Use of phones and email

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

This email account should be used for work purposes only.

Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account. Care should be taken when sharing school email addresses directly with parents – our school systems support direct emailing from central mailboxes including via our MIS, and central mailboxes should be used whenever possible.

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 Director of Finance and Operations immediately and follow our data breach procedure.

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

School phones must not be used for personal matters.

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

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The IT/Network Manager or Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no students 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 are also permitted to use mobile phones during the school day in line with the personal use guidance above. Use of other personally owned devices, including laptops, tablets etc must be requested in writing in advance and agreed by the Headteacher.

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 could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

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

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely. They should dial in using a virtual private network (VPN).

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

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Please see the data protection policy

5.4 School social media accounts

The school has an official Facebook page. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

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

5.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

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

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises

- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

6. Students

6.1 Access to ICT facilities

Students have access to ICT facilities provided by the school these include:

- Computers and equipment in the school's ICT suites are available to students 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
- School issued laptops to use under supervision of staff
- School issued laptops provided for learning at home
- Students will be provided with an account linked to the school's virtual learning environment, which they can access from any device
- Students may be able to use devices unsupervised if given permission to do so by a member of staff

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search students' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

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

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

6.3 Unacceptable use of ICT and the internet outside of school

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

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other 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 ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents

7.1 Access to ICT facilities and materials

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

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion.

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

7.2 Communicating with or about the school online

We believe it is important to model for students, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to read the Parental use of social media policy appendix 4.

8. Data security

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

8.1 Passwords

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

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

Members of staff or students who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Passwords are issued by the IT/Network Manager and may be changed by request or thought the mechanisms of the target device/software.

8.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

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

8.3 Data protection

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

Please see the 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 IT/Network Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT/Network Manager or Director of Finance and Operations immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

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

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as student information) out of school if they have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the IT/Network Manager

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security
- 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 annually, to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data to offsite location not connected to the schools network
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our MIS provider (cloud based).
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home following guidance given
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Using strong passwords and not sharing those passwords with anyone else.
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

- Work with our LA 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 internet connection is secured.

Internet access is provided on school devices and staff/visitor devices at the discretion of the IT/Network Manager.

Access to the internet is filtered and monitored. Filters may not be fool-proof therefore site that have been blocked in error or sites that have been missed can be reported to the IT/Network Manager.

10.1 Students

Students can access the internet from school devices only, all access is filtered and monitored

Students cannot access the internet on personal devices

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's internet unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's internet in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Headteacher and the IT/Network Manager 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 year.

12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Mobile phone usage

Appendix 1: Facebook cheat sheet for staff

Don’t accept friend requests from students on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your students
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your students online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or students)

Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, students 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. If the student persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Students may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

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

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use agreement (students and parents/carers)

STUDENT ACCEPTABLE USE AGREEMENT
Solway Community School and Beacon Hill Community School

- I will only use ICT systems in school, including the internet, email, digital video, mobile technologies, etc. for educational purposes.
- I will only log on to the school network/Learning Platform, other systems and resources with my own user name and password. I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username or password.
- I will follow the schools ICT security system and not reveal my passwords to anyone.
- I will only use my school email address for educational purposes. I will check my email regularly and carry out routine "housekeeping" of my email messages.
- I will not give out my personal information or that of others such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will make sure that all ICT communications with students, teachers or others is responsible, polite and sensible. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will 'log off' when leaving a computer.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will only save files to the network that are related to schoolwork. I will not use filenames that could be considered offensive.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I am aware that when I take images of students and/or staff, that I must only store and use these for school purposes and in line with school procedures and must never distribute these outside the school network without the permission of all parties involved, including in school breaks and all occasions when you are in school uniform or when otherwise representing the school.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts.
- I understand that I am responsible for my actions, both in and out of school and that the school has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement when I am out of school and where they involve my membership of the school community (e.g. cyberbullying, use of images or personal information etc.)
- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- When I am using the internet to find information, I should take care to check that the information that I access is accurate as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I will respect the privacy and ownership of others' work online at all times and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission. Where work is protected by copyright, I will not try to download copies (including music and videos).
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 only use my personal hand-held/external devices (USB devices) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- If I bring a mobile phone in to school, I must hand it in at reception at the beginning of the school day, and collect it at the end of the day
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails unless I know and trust the person or organisation that sent the email due to the risk of the attachment containing a virus or other harmful programme.
- 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.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent may be contacted and any illegal activities will be reported to the Police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this Agreement, access will not be granted to the school ICT system.

✂

Solway Community School and Beacon Hill Community School
Student Acceptable Use – Student and Parent Agreement

Dear Parent,

ICT including the internet, learning platforms, email and mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of online safety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher.

I have read, understood and agree to follow the terms of this Acceptable Use Agreement when:

- I use the school ICT systems and equipment (both in and out of school)

- I use my own equipment in school (when allowed) e.g. camera, USB stick, etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student: Class/Year Group:

Parent Signature		**Date**	
Student Signature		**Date**	

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

STAFF & VOLUNTEER

ACCEPTABLE USE POLICY AGREEMENT

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This Agreement is designed to ensure that all staff and volunteers (including Governors) are aware of their responsibilities when using any form of ICT. This applies to ICT used in school and also applies to use of school ICT systems and equipment out of school and use of personal equipment in school or in situations related to their role within the school. All staff and volunteers (where they are using technology in school) are expected to sign this Agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers are responsible users and stay safe while using technologies for educational, personal and recreational use;
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- staff are protected from potential risk from the use of ICT in their everyday work and work to ensure that young people in their care are safe users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

Keeping Safe

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will only use my own user names and passwords which will be at least 8 characters long and consist of a least three of the following: uppercase letter, lowercase letter, number, special character.
- I will not use any other person’s user name and password.
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to students.
- I will ensure that my data is regularly backed up.
- I will ensure that I ‘log off’ after my network session has finished.
- If I find an unattended machine logged on under another user’s username, I will **not** continue using the machine – I will ‘log off’ immediately.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.

- I will not accept invitations from school students to add me as a friend to their social networking sites, nor will I invite them to be friends on mine.
- As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends, especially with those connected with my responsibilities at the school, such as parents and their children.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school procedures to disclose it an appropriate authority.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the school personal data guidelines. I will not send personal information by email as it is not secure.
- Where personal data is transferred outside the secure school network, it must be encrypted or password protected. Personal data can only be taken out of school or accessed remotely when authorised, in advance, by the Head teacher or Governing Body. Personal or sensitive data taken off site in an electronic format must be encrypted, e.g. on a password secured laptop, memory stick or individual documents password protected. Staff leading a trip are expected to take relevant student information with them but this must be held securely at all times.
- I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to:
    - do not reveal confidential information about the way the school operates
    - are not confused with my school responsibilities in any way.
- I will not try to bypass the filtering and security systems in place.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

Promoting Safe Use by Learners

- I will support and promote the school’s Online Safety, Data Protection and Behaviour Policies and help students to be safe and responsible in their use of ICT and related technologies.
- I will model safe use of the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school procedures if an issue arises in school that might compromise a learner, user or school safety or if a student reports any concerns.

Communication

- I will only use the school’s email/Internet/Intranet/Learning Platform and any related technologies for professional purposes or for uses deemed ‘acceptable’ by the Head teacher or Governing Body.

- I will communicate on-line in a professional manner and tone, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. Anonymous messages are not permitted.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
- I will only communicate with students and parents using the school's approved, secure email system(s). Any such communication will be professional in tone and manner.
- I am aware that any communication could be forwarded to an employer or governors.
- I will only use chat and social networking sites that are approved by the school.
- I will not use personal email addresses on the school ICT systems unless I have permission to do so.

Research and Recreation

- I will not browse, upload, download, distribute or otherwise access any materials which are illegal, discriminatory or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity.
- I know that all school ICT is primarily intended for educational use and I will only use the systems for personal or recreational use if this is allowed by the school.

Sharing

- I will not access, copy, remove or otherwise alter any other user's file, without their permission.
- I will respect the privacy and ownership of others' work online at all times and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission, and will credit them if I use it.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos). If I am unsure about this, I will seek advice.
- Images of students and/or staff will only be taken, stored and used for professional purposes using school equipment in line with school procedures.
- I will only take images/video of students and staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them.
- If images are to be published on-line or in the media I will ensure that parental/staff permission allows this.
- I will not use my personal equipment to record images/video unless I have permission to do so from the Head teacher or other Senior Manager.
- I will not keep images and/or videos of students stored on my personal equipment unless I have permission to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that for which I have permission.
- Where these images are published by the school (e.g. on the school website/prospectus/social media), I will ensure that it is not possible in our initial

publication to identify the people who are featured by full name or other personal information.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

Buying/Selling/Gaming

- I will not use school equipment for on-line purchasing, selling or gaming unless I have permission to do so.

General Equipment Use

- Any ICT equipment issued to you remains the property of the school.
- On termination of employment/volunteering or for extended absences the school will require equipment to be returned.
- The school reserves the right to demand equipment to be returned at any time within 7 calendar days.
- I will not download or install any unapproved software, system utilities or resources that might compromise the network or are not adequately licensed.
- I will not try to alter computer settings without the appropriate permission.
- 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 not attempt to harm or destroy any equipment or data of another user or network connected to the school system.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Online Safety Coordinator or Head teacher.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

For all staff & volunteers: I understand if I do not follow these rules that this may result in loss of access to these resources.

For school employed staff only: I understand this forms part of the terms and conditions set out in my contract of employment and any breaches may result in possible disciplinary action.

✂

Staff/Volunteer Acceptable Use Agreement

I agree to use the school network and associated resources in a responsible way and observe all the restrictions as explained in the staff ICT Acceptable Use Agreement (as set out above). I agree to use ICT by these rules when:

- I use school ICT systems at school or at home when I have permission to do so
- I use my own ICT (where permitted) in school
- I use my own ICT out of school to access school sites or for activities relating to my employment or position within school.

Staff/Volunteer Name			
Job Title (where applicable)			
Signed		**Date:**	

Appendix 4 Parental use of social media

P14 Parental Use of Social Media Policy

Overview

Social networking sites such as Facebook, Twitter and other similar online forums are now widely used and these types of media allow people to communicate in ways that were not previously possible. Unfortunately, such sites can be used inappropriately by some as a means of expressing negative or offensive views about schools and their staff. This document sets out this school's approach to parental use of such sites and sets out the procedures that will be followed and action that may be taken when it is considered that parents have used such facilities inappropriately. Where there is reference to "parent" in this document this also includes carers and other relatives of a child in school.

Objectives

The purpose of this policy is to:

- Encourage social networking sites to be used in a beneficial and positive way by parents;
- Safeguard pupils, staff and anyone associated with the school from the negative effects of social networking sites;
- Safeguard the reputation of the school from unwarranted abuse on social networking sites;
- Clarify what the school considers to be appropriate and inappropriate use of social networking sites by parents;
- Set out the procedures the school will follow where it is considered that parents have inappropriately or unlawfully used social networking sites to the detriment of the school, staff, pupils or anyone else associated with the school;
- Set out the action the school will consider taking if parents make inappropriate use of social networking sites.

Appropriate use of social networking sites by parents

The school recognises that many parents and other family members will have personal social networking accounts which they might use to discuss/share views about school issues with friends and acquaintances.
However, it is not the way to raise concerns or complaints as the school will not respond to issues raised on a social networking site. If there are serious allegations being made/concerns being raised, social media or internet sites should not be used to name individuals and make abusive comments. Please contact the school to discuss any concerns you may have.

Inappropriate use of social networking sites by parents

Although social networking sites may appear to be the quickest and easiest way to express frustrations or concerns about the school and those associated with it, it is rarely appropriate to do so. Other channels such as a private and confidential discussion with Senior Staff, the Headteacher or member of the Governing Body, or using the school's formal complaints process are much better suited to this. We consider the following examples to be inappropriate uses of social networking sites. (This list is non-exhaustive and intended to provide examples only):

- Naming children or posting any comments about children who attend any of our schools;
- Making allegations about staff or anyone else connected with the school;
- Making any posts that could be deemed to be cyber-bullying;
- Making complaints about the school or staff at the school;
- Making defamatory statements about the school or staff at the school;
- Posting negative or offensive comments about staff or any other individual connected to the school;
- Posting racist comments;
- Posting comments which threaten violence;
- Posting comments or engaging in online discussions with children other than their own.

Parents should also ensure that their children are not using social networking and other internet sites in an inappropriate manner. It is expected that parents/carers explain to their children what is acceptable to post online. Parents/carers are also expected to monitor their children's online activity, including in relation to their use of social media. Please note that most social networking sites require the user to be at least 14 years old.

Procedure the school will follow if inappropriate use continues

The school will always try to deal with concerns raised by parents in a professional and appropriate manner and understands that parents may not always realise when they have used social networking sites inappropriately. Therefore, as a first step the school will usually discuss the matter with the parent to try to resolve it and to ask that the relevant information be removed from the social networking site in question. If the parent refuses to do this and continues to use social networking sites in a manner the school considers inappropriate, the school will consider taking the following action:

- Take legal advice and/or legal action where the information posted is defamatory in any way or if the circumstances warrant this;
- Set out the school's concerns to the parent in writing, giving a warning and requesting that the material in question is removed;
- Contact the police where the school feels it appropriate – for example, if it considers a crime (such as harassment) has been committed or in cases where the posting has a racial element, is considered to be grossly obscene, grossly offensive or is threatening violence;
- If the inappropriate comments have been made on a school website or online forum, the school may take action to block or restrict that individual's access to that website or forum;
- Contact the host/provider of the social networking site to complain about the content of the site and ask for removal of the information;
- Take other legal action against the individual following appropriate advice.

Appendix 5: 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.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

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

Appendix 6: School use of Social Media and Websites

In line with our Data Protection and Safeguarding and Child Protection policies, the following rules will apply when posting to social media and websites.

- Full names of children will not be used. First names (and initial of surname when essential) will be used on posts that could identify children (i.e. including photographs) and any certificates or other materials show in the photograph will only show first name, not their full name.
- Parents will be discouraged from tagging their children into posts, especially when the post includes photographs.
- Posts should be appropriately worded and spell checked.
- Access to post to our schools' facebook pages and websites is limited to Senior Leaders. Proposed communications should be sent to content editors well in advance of the proposed publication date.
- Teachers and other staff should not comment on posts that may be considered inflammatory (e.g. a post criticising the school, student or member of staff) without explicit permission from Senior Leaders. Any posts that are identified as critical or defamatory should be flagged up to the headteacher immediately.