ICT &
Internet Acceptable Use Policy

Date Approved: February 2023

Date of next review: February 2025

This policy will be reviewed at least bi-annually and/or following any updates to national and local guidance and procedures.

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 pupils, staff (including Senior Leadership Teams), Governors, Trustees, 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, pupils, parents, Governors and Trustees
- 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, behaviour and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including Governors, Trustees, staff, pupils, volunteers, contractors and visitors (including Parents and Carers).

Breaches of this policy may be dealt with under our:

- Staff code of conduct
- Parent and Carer conduct
- Behaviour policy
- Suspensions and permanent exclusions policy
- Staff discipline policy
- Safeguarding policy

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- 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
- 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
- meeting digital and technology standards in schools and colleges
- sharing nudes and semi-nudes: advice for education settings working with children and young people

3. Definitions

- **“ICT facilities”:** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones (mobile and landlines), music players or hardware, software, websites, virtual assistant technology, 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, Trustees, staff, pupils, volunteers, contractors and visitors (including Parents and Carers)
- **“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 6 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 risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school’s ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school’s ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or any other relevant member of staff of the school Senior Leadership Team and/or Trust Leadership Team 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.

Approval for such activities would be sought from the Trust CEO by the Headteacher.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's and Trust policies on behaviour, safeguarding, dealing with racist incidents, suspensions and permanent exclusions, staff discipline, staff code of conduct, parent and carer conduct. Copies of these policies can be found on the school and Trust websites.

5. Staff (including Trustees, Governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's IT facilities and services company (Gridserve) 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 service team.

5.1.1 Use of phones and email

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

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

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

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

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

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

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

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

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

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

School phones must not be used for personal matters.

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

The school can record in-coming and out-going phone conversations.

If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so.

Phone conversations are recorded:

- to aid school office administrators and Senior Leadership Teams
- for use in staff training

Staff who would like to record a phone conversation should speak to the Headteacher.

All non-standard recordings of phone conversations will be pre-approved and consent obtained from all parties involved.

The Headteacher may grant requests to record conversations when:

- Discussing a complaint raised by a Parent, Carer or member of the public
- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

5.2 Mobile phone use

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, children during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room, classrooms when children are at lunch or break etc).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time. For instance:

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members
- As part of the lockdown procedures or evacuation

The Headteacher will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact.

Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations or lockdowns
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil
- Refrain from using their phones to contact parents. If necessary, contact must be made via the school office

Staff are required to withhold their number if contacting a parent or carer in an emergency. Whenever possible staff will be provided with a school phone and/or sim card. Please refer to the Educational Visits Policy.

Some members of staff are provided with a mobile phone by the school for work purposes.

Only authorised staff are permitted to use school phones, and access to the phone must not be provided to anyone without authorisation.

Staff must:

- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet
- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct.

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while staff are travelling to and from school.

5.3 Personal use

5.3.1 ICT for 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 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 non-break 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 pupils from using the facilities for work or educational purposes

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

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

Staff are also permitted to use their personal devices (such as mobile phones, laptops or tablets) in line with the staff code of conduct, staff discipline policy, safeguarding policy and this policy

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

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

5.3.2 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.

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents, carers or pupils.

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

5.4 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Staff can access this:

- via 365 cloud
- VPN set up by the school IT services

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the network management service 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.

https://primarysite-prod-sorted.s3.amazonaws.com/galaxy-trust/UploadedDocument/41120f39-48ec-4114-86a3-75e19238b01e/data-protection-policy.pdf

5.5 School and Trust social media accounts

The school and Trust has an official Facebook, Twitter and Instagram pages, managed by school staff or the Trust communications manager. 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.

The school may 'filter and monitor' the use of ICT facilities and networks, in line with Keeping Children Safe in Education (KCSIE) guidance 2022.

Authorised personnel may raise concerns about monitored activity with the school's DSL, in line with KSCIE 2022

5.6 Monitoring of school and Trust network and use of ICT facilities

The school and Trust reserve 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 and Trust monitors ICT use in order to:

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

6. Pupils

6.1 Access to ICT facilities

ICT facilities available to pupils:

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology etc must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment such as Outlook 365, which they can access from any device.

6.2 Search and deletion

Under the Education Act 1996, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

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

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

6.3 Unacceptable use of mobile phones, ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, dealing with racist incidents policy and suspensions and permanent exclusion policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

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

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

6.4 Mobile Phones

Only children in Years 5 or 6 are permitted to bring mobiles phones to our schools with parental permission.

Children are permitted to bring phones in to school if:

- Travelling to school by themselves
- The child is a Young carers who need to be contactable

Pupils are allowed to bring phones to school, but not use them during the school day, and they must be stored with the designated adult within the school. Pupils must adhere to the school's code of conduct and acceptable use agreement] for mobile phone use (see appendix 3 & 4).

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

6.5 Sanctions

If a pupil breaches this policy

- Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006)
- If they are confiscated, a parent or carer will be able to collect the item from school once a meeting has been arranged with a member of the Senior Leadership Team.
- Sanctions for unacceptable use link with the Trust behaviour policies

Staff also have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation. The DfE guidance allows the school to search a pupil's phone if we have reason to believe the phone contains pornographic images, or if it is being or has been used to commit an offence or cause personal injury.

If inappropriate content is found on a phone, school ICT equipment or if there is suspect inappropriate behaviour, the Trust behaviour and safeguarding policies will be applied.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies such as Childrens Social Care as appropriate.

Such conduct includes, but is not limited to:

- Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
- Upskirting
- Threats of violence or assault

- Abusive calls, emails, social media posts or texts directed at someone based on someone's ethnicity, religious beliefs or sexual orientation

7. Parents

7.1 Access to ICT facilities and materials

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

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

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

7.2 Communicating with or about the school online

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

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

We ask parents and carers to sign the agreement in appendix 2.

7.3 Use of mobile phones by parents, volunteers and visitors

Parents, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's a public event (such as a school fair), or of their own child
- Using any photographs or recordings for personal use only, and not posting on social media without consent
- Not using phones in lessons, or when working with pupils

Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents
- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

Parents or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in this policy.

Parents must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on his/her personal mobile during the school day.

The school will ensure that it communicates with parents and Carers about pupil activity, in line with KSCIE 2022.

8. Data security

The school and Trust are responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user

accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times. The Trust will use the government's digital and technology standards in schools and colleges.

8.1 Passwords

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

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. This includes personal mobile phone security.

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

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

8.2 Software updates, firewalls, and anti-virus software

All the school and Trust 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 Trust's data protection policy.

The policy can be found on the school and Trust's website

8.4 Access to facilities and materials

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

These access rights are managed by Gridserve.

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 Gridserve 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 Trust ensures that all devices and systems have an appropriate level of encryption.

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

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT service provider, Gridserve and/or Cantium.

9. Protection from cyber attacks

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

The Trust and its schools will:

- Work with Trustees, Governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this using a third-party audit (such as this one) 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 regularly, ideally at least once a day through the Trust's automatic systems and store these backups on cloud based backup systems and/or external hard drives that aren't connected to the school network and which can be stored off the school premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider and our IT service providers.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure 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 at least annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Schools will work with the Trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The Trust wireless internet connection is secured through:

- The use of filtering
- Separate connections for staff, pupils, parents and the public

We are aware that filters aren't fool proof. All stakeholders should report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the relevant member of IT staff or Grid serve.

10.1 Pupils

Trust approach to the use of Wi-Fi by pupils, consists of:

- The use of filtering for security
- Wi-Fi access on school grounds for accessibility
- Password protected devices
- Supervision by staff when accessing the internet

10.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi 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 Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

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

11. Monitoring and review

The Headteacher, Central leadership team and network providers 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.

12. Related policies

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

- Safeguarding and child protection
- Behaviour including Suspensions and permanent exclusion and Dealing with Racist incidents policies
- Staff discipline and code of conduct
- Data protection
- Educational Visits
- Remote education in line with KCSIE 2022

Appendix 1: Facebook cheat sheet for staff

Don’t accept friend requests from pupils on social media!

10 rules for school staff on Social Media

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

Check your privacy settings

- Change the visibility of your posts and photos to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list
- Don’t forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture

- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

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

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

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or 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 of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook, Twitter and Instagram page • Email/text groups for parents (for school announcements and information) • Our virtual learning platform such as Dojo, 365 Office etc Parents and carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure I will not: • Use private groups, the school's social media pages, or personal social media to complain about or criticise members of staff. This is not constructive and the school cannot improve or address issues if they are not raised in an appropriate way • Use private groups, the school's social media pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I am aware of a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the mobile phones, school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using my mobile phone, the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Keep my mobile in my possession but give it to the designated adult when I arrive at school
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- Share my passwords with others or log in to the school's network using someone else's details
- Bully other people

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (such as computers and equipment) and use the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and ensure that I am following the rules.

I will tell a teacher or a member of staff immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I am not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, Trustees, Governors, volunteers and visitors

Acceptable use of mobile phones, the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using mobile phones, the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms on school ICT equipment • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify, delete or share data I'm not authorised to access, modify, delete or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will immediately let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the 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.
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.

TERM	DEFINITION
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.