POLICY: Acceptable use of ICT and Internet policy (incorporating online safety)

STATUTORY: Yes

DATE AGREED: March 2025

REVIEW DATE: March 2028

RESPONSIBLE MEMBER OF STAFF: A Williams

GOVERNOR COMMITTEE: FGB

SIGNED HEADTEACHER: J Holmes

SIGNED CHAIR OF GOVERNORS: R Whitehouse

Contents

1. 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 the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

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

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

This policy also aims to capture, reinforce and condense the relevant sections of the school code of conduct which outline rules for staff (in all capacities and descriptions) in terms of communicating with students online, maintaining data security and confidentiality, plus use of school online resources.

This policy also aims to capture, reinforce and condense the Hoople policy on "social media" which the school defaults to regarding the use and misuse of social media platforms in and outside of school by staff (in all capacities and descriptions)

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

Breaches of this policy may be dealt with under our disciplinary policy (staff) and behaviour policy (students)

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- C**onduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1.2. Scope of policy

The scope of this policy applies to all staff including teaching and support staff,contractors , volunteers . It applies to both permanent and temporary school contracts and placements. In terms of students it covers all young people from Year 7 until Year 13 and in areas such as online communication it extends to ex students.If staff believe there is both credible and justified reason to have online discourse with a post 18 years student using personal (not school) online messaging and communication., they should notify and discuss this with the DSL . This guidance extends to periods of home/virtual learning and also to the school holidays.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to:

- 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
- 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)
- Online Safety Act 2023
- Education and Training (Welfare of Children Act) 2021

The guidance also reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study and the Education for a Connected World framework - 2020 edition. Policy complies with our funding agreement and articles of association.

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, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the 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

4. Roles and responsibilities

4.1. The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

Governors will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Review this policy with stakeholders such as the lead teacher for online safety and the DSL as part of an overall review of online safety

4.2. The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. He also has overall responsibility assisted by the Human Resources manager and external advisors in the management and response of all staff allegations including those risen as "low level concerns"

4.3. The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

- The DSL takes lead responsibility for online safety in school, in particular:
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Line managing and supporting the work of the online safety lead teacher
- Ensuring that an adequate – and statutory- level of filtering of school Internet use is in place

This list is not intended to be exhaustive.

4.4. The lead teacher of online safety

The lead teacher of online safety is responsible for:

- Planning & producing E-safety lessons for the PSHE curriculum.
- Planning & producing E-safety lessons for the Computing KS3 curriculum.
- Approving & producing online safety workshops.
- Planning & monitoring the implementation of the KS4 cross curricular computing scheme of work.
- Liaising with year leaders and the DSL lead to provide information for parental and staff emails.
- To assist in the production of school policies that focus on the use of computers.
- To provide up to date advice and information to parents

4.5. The ICT/Network manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

4.6. All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and subsequent updates
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use. This includes not sharing personal data, contact details and information online with students and not engaging with students online using personal email/ mobile phone/camera devices/ gaming systems and or other online platforms (using school email and Epraise only) It also sates that staff should follow all guidance on file security and password protection plus should avoid using school online systems for personal use and storage of personal data. It goes on to state that privacy settings should be installed and reviewed by all staff with personal online accounts and devices plus personal mobile devices should be kept secure and for the most out of site at school
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Report any possible personal breaches of this policy and indeed any concerning online behaviour of students they may encounter to the DSL
- Report any concerns they may have about other staff and there unacceptable use of ICT systems and online technologies to the headteacher either as a low level concern or IF their concern meets one of the 4 thresholds of harm outlined in KCSIE as a significant and urgent concern
- To use secure email systems and student initials rather than full names as and when directed by the DSL and deputies who may request that you communicate and update stakeholders about particular students for example using My Concern, Anycomms or Egress

This list is not intended to be exhaustive.

4.7. Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

Parents/Carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Saferschools app

4.8. Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

5. 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

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 the IT Manager
- 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 of the IT Manager
- 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 IT 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.

The school will highlight and signpost for parents/carers appropriate organisations and sources of information regarding online safety in terms of online CONTENT, CONTACT CONDUCT and COMMERCE in line with organisations recommended in KCSIE 2021 Annex D

Through PSHE, ICT lessons and the assembly programme the school will also seek to prevent both harmful and unacceptable uses of Communication technologies in terms of accessing CONTENT, making inappropriate and potentially harmful CONTACT, their personal CONDUCT and the risks of COMMERCIAL activities posed top young people

5.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies.

6. 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.

Whereby an exception to the acceptable use conditions highlighted above potentially involves a breach to the child protection policy in terms of safe use or is in contradiction of sections 126-135 of Keeping Children Safe in Education then advice must be sought from the DSL

IT Manager check access to prohibited sites as part of system security.

7. Pupils

7.1. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum of PSHE, the assembly programme and Computer Science.

The schools approach to teaching online safety is based on the Teaching online safety in schools government guidance & the Education for a Connected World government guidance. The School is mapping the content taught against the Education for a Connected World framework.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns Pupils

in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- Phishing, identity theft, extremism, conspiracy theories , fake news, online dares and challenges.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

7.2 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 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.

7.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises) and will reserve the its right and duty to notify other stakeholders including the police and or children's services if there is any indication of Child protection issues or Peer on Peer abuse.

- 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, or 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

7.4. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during their time on school site. Unless they have asked a member of staff for permission and have been granted permission under extenuating circumstances.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which will result in the confiscation of their device and an after school detention.

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 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.

8. Parents and carers

8.1 Access to ICT facilities and materials

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

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

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

8.2 Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

- Through the Safer schools app.
- Through communications and updates on the parent pay portal.
- Online safety will also be covered during Y6 school induction parents' evening.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised through the schools complaints policy.

9. Cyber-bullying

9.1. Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

9.2. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups as part of PSHE.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes Computer science and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training..

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all appropriate endeavours to ensure the incident is resolved.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

9.3. Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

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

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the DSL should reasonably suspect that the device has, or could be used to:

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

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

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

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

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

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

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

The school's IT Manager 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 Manager

10.1. 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. 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 protected 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 School Business Manager 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 7.4.

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

10.2. Personal use

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 7.5.5). Where breaches of this policy are found, disciplinary action may be taken.

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

10.3. Personal social media accounts

Members of staff should ensure their personal use of social media is appropriate at all times. Staff are expected to ensure that any social network privacy settings maintain their professionalism and do not compromise or tarnish the reputation of John Masefield High School. Accounts should be secured in order that pupils cannot easily access them.

- Staff are permitted to be 'friends' with ex-students once the student has reached the age of 21.
- Staff are permitted to be 'friends' with their own children or those for whom they have parental or official carer responsibility
- It is accepted that staff may be 'friends' with parents on social networking sites before their children attend JMHS. The requirement is that staff are always mindful of their professional responsibility to JMHS when using social networking sites.

10.4. Remote access

We allow staff to access the school's ICT facilities and materials remotely using Citrix Workspace. 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 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. Our Data Protection policy can be found on our website, (About Us/Policies)

10.5 School social media accounts

Neither staff or pupils should create or use social media accounts on behalf of the school without permission of the School Business Manager

10.6 Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10.7 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 and 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 and for the safeguarding of staff and pupils
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

11. Social Media

The following information paraphrases and is in accordance with the Hoople Social Media policy employed by the school. The school for this purpose defines " social media" as any online platform that has the potential to or routinely makes available information and communications to the general public. It also here extends to online blogs, product ratings, web forums, photo posting boards, message boards and gaming systems.

11.1. Staff

Staff must refrain from knowingly engaging with students on such forums and should report such incidents. They must also refrain from posting any material which could be considered sexual, illegal or offensive regardless if a student has or has not seen it. They should also not post anything which could breach copyright or data protection laws or be interpreted to be endorsing a particular product or political ideology especially if views are not clearly stated as yours and only yours (not reflecting the position of the school).

In summary staff should avoid any online communication that may bring the school into disrepute even only if it was misconstrued.

Staff should not seek to use social media as a learning tool unless they have clearance from the DSL and Network manager to do so.

Staff should assume that everything posted on “social media” platforms is permanent and publicly available plus can be used in disciplinary actions/responses.

11.2. Student

Students should not seek out staff members social media profiles, or attempt to follow, subscribe or add as a friend a member of the school staff. All attempts will be reported to the DSL team and sanctions may be applied.

Students will not make false online profiles under the name of students or staff, all attempts will be reported to the DSL team and sanctions may be applied. In most cases, the online impersonation is likely to result in the impersonator committing criminal acts and civil wrongdoings. Civil wrongdoings would usually include breach of privacy, misuse of private information, defamation and harassment.

Students will not attempt to take photos/videos while on school site to be uploaded to social media sites, All attempts will be reported to the DSL team and sanctions may be applied.

Where pupils are found to have made malicious or unfounded claims against staff, appropriate disciplinary processes may be actioned, treated similarly to cases of physical assaults.

11.3. 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, pupils, parents and others who use the school’s ICT facilities should use safe computing practices at all times.

11.4 Passwords

All users of the school’s ICT facilities should set strong passwords for their accounts and keep these passwords secure. Passwords should be at least 10 characters long and consist of lowercase, upper case letters and numbers. Pass phrases consisting of random words are easier to remember and secure if at least 10 characters long.

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

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

Staff are recommended to use a password manager to help them store their passwords securely. Passwords must not be reused over multiple services and certainly the same password must not be used to access both school and home services.

11.5 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.

11.6 Data protection

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

Our Data Protection policy can be found on our website, (About Us/Policies)

11.7 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 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 Manager immediately.

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

USB drives are not endorsed, Remote Access being the recommended method of working remotely. If USB drives are used, no personal data may be copied to them at any time and their use must be restricted to storing resources and material for teaching and learning.

12. Protection from cyber attacks

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, 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 (360 Degree Safe (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 overnight. These backups on cloud-based backup systems and immutable local storage located separately from the server room.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to IT Manager
- Make sure staff:
    - Connect to our network using a Citrix secure connection via Netscaler when working from home
    - 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'

13. Wi-Fi

Wi-Fi is available across the site for staff to connect their mobile devices and to provide a connection to the 3CX phone system from their mobile phones.

13.1 Pupils

- Wi-Fi is available in the VI Form, where students are allowed to connect their personal devices. The VI Form Wi-Fi is segregated from the school network and provides internet access solely, through which the school IT resources may be accessed via Citrix Remote Access

13.2 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 IT Manager.

The IT Manager will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer)
- 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.

14. Virtual learning arrangements

14.1. This element of the policy aims to:

- Ensure consistency in the school's approach to virtual communication, live streamed lessons.
- Set out expectations for all members of the school community with regards to live streaming lessons.
- Provide appropriate guidelines for data protection.

14.2. Remote Learning Arrangements and video calls

- All live lessons and video calls must be carried out during the normal timetable; there must be no lessons held outside of normal class hours.
- Live streaming, video call lessons must only be conducted using the agreed platform for JMHS this is Microsoft Teams. Teachers may choose to use a number of additional tools to support students. The learning platform selected is due to many considerations, such as being able to use school email accounts, the safeguarding of personal data, privacy questions and policies, and terms of service.
- If a department already uses other methods of communication and online platforms that the JMHS has supported, these may continue to be used for remote learning. It is important for staff to observe the requirement that unless permission has been granted, other methods of communication must not be used.
- Live streaming lessons must only be for pupils on roll at the school and delivered by teachers working at the school. Lessons will be by invitation only and teachers will initiate and close lessons. Pupils will be invited to participate in a lesson by their school email address. Only school-registered email accounts must be used. Personal accounts of either the pupil or teacher must not be used.
- School staff are able to use personal devices if all protocols are followed.
- Lessons and video calls should be conducted as though they were taking place at the school premises. The teacher must be aware of their surroundings when recording a lesson. This must be in an appropriate place and suitable environment, not in a bedroom or where inappropriate objects or information is visible.
- Where teaching is being undertaken remotely from home, it is important that the teacher ensures the security of any devices being used, for example ensure the camera is switched off when not in use, ensure meetings are closed down when finished, ensure microphone is muted when not speaking. Ensure antivirus software is up to date.
- The staff member must consider carefully any resources to be used. Use of online webpages in school will be subject to internet content filtering and is unlikely to be replicated in the home environment.
- The staff present are expected to maintain professional teaching standards at all times. All staff are expected to exhibit high standards of professional conduct, language, behaviour and attire, in compliance with the Staff Code of Conduct.
- The school's ICT and internet acceptable use policy continue to apply to the pupil and the teacher. Staff must not post or 'broadcast' anything that will bring them, the school into disrepute. The staff member leading the session must ensure that the pupil is reminded about the policy.
- The Head teacher or other senior leaders must conduct spot monitoring of remote lessons to check compliance.
- The school must notify the parent that the sessions will be taking place, providing advance notice. The parent must be advised not to join the session, unless it has been agreed in advance with the parent by the person delivering the lesson. This will enable pupils that have special educational needs or younger aged pupils to be supported by the parent. The parent must have signed to say they have read and understand the school's expectations around live streaming.
- Staff must be aware that some students will not enjoy or adapt well to a remote learning method. Those who are already anxious, who have less understanding of technology or who find it hard to concentrate on tasks may struggle to engage or simply find the whole lesson overwhelming.
- Before commencing a live learning session, the staff member leading the session must have considered whether some pupils will be excluded from the lesson owing to a lack of resources. They must provide alternative learning where this is the case.
- For pupils subject to safeguarding thresholds, a risk assessment must be undertaken by the Designated Safeguarding Lead (DSL) before the pupil participates in the session. The class teacher must inform the DSL that a session will take place, whether this is by pre-recorded or by live streaming means.
- The member of staff leading the session should ensure that a record of attendance of all pupils attending the live streaming session is available on request.

- Both the staff member and the pupil must turn off all notifications on their device used for lessons to avoid disruption, unsolicited pop-ups and exposure of personal data, otherwise the lesson cannot take place. It is the staff member's responsibility to remind the pupil to do so.
- Where there is disruption to a lesson due to unsolicited pop-ups or exposure of personal data, the lesson must be immediately discontinued and the Head teacher or other senior leader and Designated Safeguarding Lead notified. The Safeguarding and Child Protection Policy and the General Data Protection Regulations Policy must be applied as required. All incidents and actions must be recorded on the school's safeguarding system.
- If a pupil account is not working, for example, the pupil has a problem accessing school webmail or they get locked out and no solution can be found, they are to contact the school administration office.
- If a parent has concerns about any aspect of a lesson or video call they should contact the school directly to discuss it and not raise issues during the lesson itself. All concerns and complaints are taken very seriously
- The staff member must establish the expectations for the virtual classroom.
- This must include how the pupil can ask questions and when to speak.
- Pupil behaviour must be in accordance with the school's Behaviour Policy.
- Where there is non-compliance to the policy, the teacher must deal with matters as if the lesson is taking place in the school setting. All incidents must be reported to the Head teacher or senior leader and Designated Safeguarding Lead. Information must be recorded on the school's safeguarding recording system.
- If there is an unauthorised person in the lesson, the teacher must discontinue the lesson, unless to do so would increase the risk of harm to the child. The teacher must immediately inform the Head teacher or senior leader and Designated Safeguarding Lead. The school Child Protection Policy must be followed. Information must be recorded on the school's safeguarding recording system.
- If the teacher is concerned about the welfare of the pupil during the lesson or video call, this must be immediately reported to the Designated Safeguarding Lead. Where possible, the teacher must continue with the remote session to allow the DSL to assess the situation, unless to do so would increase the risk of harm to the child. The school Child Protection Policy must be followed. Information must be recorded on the school's safeguarding recording system.

15. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

17. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using the My Concern safeguarding platform. Concerns re staff and the misuse of online facilities is held with the headteacher

The headteacher and IT 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 3 years.

18. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy
- Hoople Social Media Policy
- School code of conduct

Appendices:

Appendix 1: Student Summary of Online Safety Policy

Pupil Online Safety Policy Summary

When using the school's ICT facilities (like computers and equipment) and get on the internet in school, you cannot:

- 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 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

The school will check the websites you visit and how you use the school's computers and equipment. This is so that they can help keep you safe and make sure your following the rules.

You should tell a teacher or a member of staff immediately if you find anything on a school computer or online that upsets you, or that you know is mean or wrong.

The schools Wi-Fi is for staff and sixth form use only.

You cannot use your mobile phone while on school grounds (unless you have asked a staff member and supervised while using it). If you are seen using your phone it will be confiscated by school staff and held in the house office until end of day, you will also have an automatic after school detention

You will be taught online safety in your Computing, PSHE lessons and via workshops with your head of year.

You should not attempt to contact/follow/subscribe to staff members social media profiles.

If required online lessons will be conducted via Teams, registers will be taken.

The school can discipline you if I do certain unacceptable things online, even if you are not in school when you do them.

Appendix 2: Parent/Carers Summary of Online Safety Policy

Parent/Carers Online Safety Policy Summary

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

The school will raise parents' awareness of internet safety via:

- letters or other communications home.
- Information via our website.
- Through the Safer schools app.
- Through communications and updates on the parent pay portal.
-

The schools Wi-Fi is for staff and sixth-form use only, it is up to the IT manager if volunteers are given access.

Students are not allowed to use mobile phones or smart watches (for communication/gaming purposes) while on school site unless they have asked staff members permission beforehand, if they break this rule their phone will be held to the end of the school day by their year leader. You will then be contacted for the booking of an after-school detention.

If remote learning is to be undertaken you will be informed ahead of time via Email from the headmaster informing you of how it will be taking place.

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 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

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- support for parents and carers to keep children safe from online harm which provides extensive resources to help keep children safe online and details of specific online risks, including sexual abuse, criminal exploitation and radicalisation
- CEOP Education provides advice from the NCA on staying safe online
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support

- Internet matters provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- London Grid for Learning (LGfL) has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

- Keeping children safe online has support for parents and carers from the NSPCC, including guides on social media, internet connected devices and toys and online games.
- Let's Talk About It has advice for parents and carers to keep children safe from online radicalisation
- UK Safer Internet Centre has tips, advice, guides, and other resources to help keep children safe online, including parental controls offered by home internet providers and safety tools on social networks and other online services
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- School website section on online safety support
- Saferschools app

Appendix 3: Staff Summary of Online Safety Policy

Staff Online Safety Policy Summary

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and subsequent updates
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use. This includes not sharing personal data, contact details and information online with students and not engaging with students online using personal email/ mobile phone/camera devices/ gaming systems and or other online platforms (using school email and Epraise only) It also sates that staff should follow all guidance on file security and password protection plus should avoid using school online systems for personal use and storage of personal data. It goes on to state that privacy settings should be installed and reviewed by all staff with personal online accounts and devices plus personal mobile devices should be kept secure and for the most out of site at school
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Report any possible personal breaches of this policy and indeed any concerning online behaviour of students they may encounter to the DSL
- Report any concerns they may have about other staff and there unacceptable use of ICT systems and online technologies to the headteacher either as a low level concern or IF their concern meets one of the 4 thresholds of harm outlined in KCSIE as a significant and urgent concern
- To use secure email systems and student initials rather than full names as and when directed by the DSL and deputies who may request that you communicate and update stakeholders about particular students for example using My Concern, Anycomms or Egress
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Computer science and other subjects where appropriate.

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

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Staff must refrain from knowingly engaging with students on such forums and should report such incidents. They must also refrain from posting any material which could be considered sexual, illegal or offensive regardless if a student has or has not seen it. They should also not post anything which could breach copyright or data protection laws or be interpreted to be endorsing a particular product or political ideology especially if views are not clearly stated as yours and only yours (not reflecting the position of the school).

- In summary staff should avoid any online communication that may bring the school into disrepute even only if it was misconstrued.

- Staff should not seek to use social media as a learning tool unless they have clearance from the DSL and Network manager to do so.
- Staff should assume that everything posted on “social media” platforms is permanent and publicly available plus can be used in disciplinary actions/responses.

The school provided email address.

- This email account should be used for work purposes only. 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 protected 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 School Business Manager 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 7.4.
- If staff record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so, normally for safeguarding reasons.

Personal use.

- 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 7.5.5). Where breaches of this policy are found, disciplinary action may be taken.
- Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Remote learning.

- Where teaching is being undertaken remotely from home, it is important that the teacher ensures the security of any devices being used, for example ensure the camera is switched off when not in use, ensure meetings are closed down when finished, ensure microphone is muted when not speaking. Ensure antivirus software is up to date.

- The staff member must consider carefully any resources to be used. Use of online webpages in school will be subject to internet content filtering and is unlikely to be replicated in the home environment.
- The staff present are expected to maintain professional teaching standards at all times. All staff are expected to exhibit high standards of professional conduct, language, behaviour and attire, in compliance with the Staff Code of Conduct.
- The school's ICT and internet acceptable use policy continue to apply to the pupil and the teacher. Staff must not post or 'broadcast' anything that will bring them, the school into disrepute. The staff member leading the session must ensure that the pupil is reminded about the policy.

Acceptable use and online safety policy version log

Version	Date	Completed by	Comment	Approval
2.0	March 2025	J Holmes	Update names of personnel in post Update links and reference to legislation and policies	FGB March 2025