Mount Carmel

R.C. HIGH SCHOOL

Digital Communications Policy

Last review date: July 2024 – Mr B Georgy

Next review date: July 2025 – Mr B Georgy

A Family of Faith & Learning

Digital Communications Policy 2024-25

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This policy is set out to establish best practice within school and ensure fair use of technology by all partners within Mount Carmel RC High School.

All parties within Mount Carmel RC High School should follow this policy when using the ICT systems provided within school and outside of school to keep a high level of professionalism.

Contents

1. Staff Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible IT users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school reserves the right to monitor and record my use of the school digital technology and communications systems, including CCTV email and voice communications.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Edulink etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. Staff are permitted to use IT facilities for personal use at the discretion of the headteacher but must abide by the Acceptable Use Agreement and Digital Communications Policy at all times.
- I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may see this and gain unauthorised access, for example sticky notes or notepads.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will abide by the school’s Digital Communications Policy at all times.

- I understand the school's IT infrastructure may be shutdown after normal school hours to help conserve energy, in most cases this will be 6pm. Anyone still wishing to use the IT systems after this time may do so but must ensure all work is saved by 6pm and ensure the equipment is properly shutdown after use.
- I understand there may be disruption to the school IT systems at certain times in order to carry out planned or emergency maintenance in the interest of network security. The Network Manager will normally carry these tasks out during school holidays to minimise disruption however in certain cases it may be required to complete this during normal school hours.

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

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their / their parents' or carers' permission. I will record these images in line with the schools Digital Communications Policy. Where these images are published (e.g. on the school website / social media) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems i.e. your Mount Carmel assigned email address or via Edulink/ School SMS. Any such communication will be professional in tone and manner. I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

- I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have permission from the Network Manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in school Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Multi-Factor Authentication and account security:

In line with the Department for Education standards, we require staff to setup 2-factor authentication in order to protect accounts and the confidential data they have access to. Multi-Factor Authentication helps secure accounts by providing and extra layer of security, should someone gain unauthorised access to the account, the staff member would have to approve this login via the authentication app. MFA can be achieved by installing the "Microsoft Authenticator" app on a personal or school owned device and following the instructions given from the Network Manager.

- I understand that multi-factor authentication is required on my account for security purposes.
- I will only approve logins that I have initiated.
- If I lose access to my device or have a new device, I must liaise with the IT Support team to setup another device.

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

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

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

- I understand that this Acceptable Use Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

- I understand the school may exercise its right to monitor and ensure transparency in the use of the school's information systems and Internet access to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

- I understand that the use of computer systems & telecommunications systems, including browsing history and phone calls are monitored and stored for up to 90 days in line with our Digital Communications Policy. The school may exercise its right to monitor and ensure transparency in the use of the school's information systems and Internet access to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place. In certain cases, we may be required to share this information with the relevant authorities as required by law.

2. Email and Digital Messaging

The proliferation of email traffic over the last few years has allowed us to communicate more efficiently and effectively. We are entering an even greater period of email use as students and parents now also have the ability to benefit from this form of communication. In order to ensure that all parties (staff, pupils and parents) continue to find email use effective and not too burdensome, we ask that the guidelines listed below are adhered to.

Email etiquette

- Try to decide if you are sending an email for the purposes of information giving, or for some other reason. Information giving is definitely the best use of email - but be careful with any other purpose, particularly any that involves emotion!

- Avoid using email for complaining or venting – this is not an appropriate use of the medium. Don't use email as an excuse to avoid personal contact. A simple 'rule of thumb' is to ask yourself if you would say what you have written directly to the person.

- Humour can also be easily misinterpreted, especially sarcasm. Try to avoid it unless you know the recipient very well.

- Try to keep the email as a whole brief, and to include a clear subject line as a header so people can identify swiftly whether or not it is relevant to them.

- Double check everything you write, as errors can be harder to spot at certain times of the day, when you are rushing or when you are occupied by other things.

- Check to whom you are sending the email before sending it. Bear in mind that the 'Reply to all' option should only be selected if you really need everyone on the distribution list to see your reply. This should be used sparingly.

- Please also think carefully before using the CC option. Only use it when necessary and in the understanding that it does not require a direct response but is for background information only.

- If you are writing about more than one subject, do so in separate emails to avoid confusion. Messages are more easily missed if embedded in a long, wide-ranging missive. The best approach is to re-read your email to check for clarity before you send it.

- Make sure that you are clear as to what the purpose of the email is. Do you require specific action, or is the email for information only?

- If the email you are sending requires specific action you should ensure that it is sent a minimum of 24 hours* (or 48 hours* where substantive action is needed) in advance of any deadline so that the recipient(s) are given sufficient notice.
  *Excludes weekends.

- Please note that defamatory or abusive emails should not be responded to. The receipt of such emails should be reported to your line manager and the Network Manager if from external sources.

- Be careful when forwarding or replying to email threads, especially between numerous parties. When forwarding or replying to an email, be mindful of potentially sensitive information or comments within email threads that may not be intended for all recipients.

<u>Staff email</u>

To staff

Why? Think carefully about whether you actually need to send that email, sometimes we are just shifting work from ourselves to others. Can the answer be found through some other means? Would waiting until you can speak in person actually be more effective?

When? **Staff should, where possible, avoid sending any emails before 7.30am and after 5pm on weekdays.** Staff should avoid sending emails during the weekend unless absolutely necessary. Many of us choose to work outside these times but it is very easy to save the email in draft form. You can then send your drafts the next day. It is also possible to schedule an email to be sent within these times.

Who? Avoid sending emails to staff members to whom it is not relevant. It is easy to set up email groups if you regularly send emails to specific groups of staff. **Please try not to use the 'All Staff' email unless it is absolutely necessary** - the noticeboard in the staffroom or staff briefing might be more appropriate. We also have specific email groups set up for teachers and non-teaching staff which may be used where appropriate. **When replying to emails please be careful not to select the 'REPLY ALL' option (unless necessary to do so)** but click the drop-down arrow and select reply and add any intended recipients.

To pupils
Why? Email is a great way to send resources to pupils and to collect work from them. Ensure that you are clear with your pupils about what constitutes appropriate email use, for example that formal language and protocols are adhered to. Avoid responding to straightforward pupil requests. It is important that pupils still come and speak to us if they have an issue and don't just fill up staff inboxes with simple questions.

When? Be careful not to email pupils outside the school day or when they are engaged in someone else's lesson. Again, this can be avoided by saving emails to draft and sending them when you have the pupils with you, before school or at lunch time, or when staff are free. This will avoid disturbing other teachers' lessons.

Staff should ensure that they use pupils' school email addresses ONLY. The use of personal addresses would leave staff members extremely vulnerable. Therefore, for the protection of members of staff, pupils' personal email addresses MUST NOT be used.

To parents
Digital Messages sent to parents and other external bodies should always be highly professional and formal in their content and tone. Full contact details should be included so that parents know with whom they are communicating - particularly if out of normal school hours.

As far as possible, digital communication with parents should be positive. If there is any sensitive information to share, communication should be undertaken either by phone or, preferably, face to face via a meeting organised specifically to address concerns.

Pupil to staff email
Pupils should make sure that they use the school email addresses of staff members at all times, and NEVER their personal ones. They should also consider whether it is really necessary to be contacting staff in this way - would it be more appropriate to see them face to face at the next opportunity? Email should not be used as an excuse by pupils to avoid speaking to their teachers.

The best use of email is for simple, factual information - emailing staff is a privilege not to be abused and should be treated as such. Pupils should ensure that basic rules of politeness are maintained.

Parent to staff email
When a concern or query arises, parents should communicate with the Curriculum Leader or Head of Year in the first instance either by telephone through the school office, or by using the 'Contact Us' page on the school website.

Parents are requested not to email members of staff directly even if their email addresses are known, unless there is a pre-agreed arrangement between the teacher and the parent. If parents are unsure as to how to direct a website message, they should contact the main office for assistance. Parents should include their child’s name and form in the message, as well as the phone number upon which they wish to be contacted.

We request that parents refer all school-related matters back to the school, and do not approach other pupils or contact other parents directly about such issues. We are interested in working with parents to create solutions. Contacting other pupils or parents can complicate and even exacerbate problems, whereas referring a concern immediately to school will expedite a resolution. If parents have a complaint to make, they should contact the appropriate Curriculum Leader to discuss the best way in which to do this. The parent may be asked to put his or her concerns in writing. If so, an email to the appropriate person would be an efficient way in which to do this. Should parent to staff communication become abusive, unreasonably persistent, or vexatious, school will follow the steps set out in the Parental Communications Policy.

Due to the difficulties of arranging interviews with teachers during the timetabled teaching day, parents are requested to seek a mutually convenient meeting time with the staff member involved to discuss concerns. It is recommended that parents suggest two or three possible times at which they can be available, and members of staff will reply at their earliest convenience.

Chain Mail
Staff should avoid sending chain mails like jokes, funny images etc. The sending of such emails is highly inappropriate and unprofessional in the workplace.

Spam/Phishing Emails
Any emails received asking you to ‘Check your account’ or ‘Provide bank details’ are more than likely malicious emailed designed to gain access to your accounts or bank accounts, emails like this should be deleted immediately. **Do Not Click Any Hyperlinks.** If anybody is unsure, please forward to the Network Manager and they will advise accordingly.

Periodic ‘Phishing’ tests will be sent out by the Network Manager, anyone who fails these tests will be required to partake in extra awareness training at the headteachers discretion.

Email on Mobile Devices

Where possible staff should refrain from having emails on mobile devices to minimise the risk of a data breach and to assist with having a healthy work/life balance.

If staff are to use email on mobile devices, email should only be used on a password protected device.

Staff should only access emails via the official **Microsoft Outlook** app available on both Apple Store and Google Play.

Staff are not permitted to have access to emails on their mobile devices if a device password is not set.

If staff lose their mobile device containing school emails, whether personal or school owned device, staff **must** report this to the Data Protection office and Network Manager immediately, no later than 24 hours.

Mount Carmel RC High School reserve the right to remotely wipe ANY mobile device containing Work emails, for the purpose of preventing a data breach, for example a lost or stolen phone. By using work emails on your phone, you agree to these conditions.

3. Digital Storage and Data Retention

Data Storage

Information Technology and computers have become vital within the education sector over the past few years, and as the demand for technology increases, so does the need for larger data storage solutions.

Although we have adequate resources in place, staff should be mindful of how much storage they are consuming on the network as it is a finite resource shared across the school.

Staff should follow these rules along with the ***ICT Acceptable Use Agreement***

- Personal files with no relation to work such as photos, videos, movies, MP3s and other files are not permitted on the network. These can be stored on OneDrive for backup if required.
- Backups of Pen drives are not permitted on the network.
- Illegal or copyrighted materials must not be stored on the network.
- Staff should delete old files no longer required, especially photos and videos of past pupils.
- The IT department reserve the right to remove any files from shared areas that they may deem confidential or should not be shared amongst staff.
- Photos of students should be stored in the 'Staff Shared Area' under 'Student photos' in their correct year/folder.
- The 'Staff Shared Area' (sharepoint) is for the storing of files which need to be shared to staff, e.g. policies, IEPs etc, all personal files should be stored in your Onedrive folder.
- Confidential data should not be shared on Staff Shared Area, unless absolutely necessary and if this is highly confidential, you should liaise with the IT Department before doing so, who can advise and help with storing in a specific, rights-protected folder.
- At the end of each term, staff should delete any unwanted files they know they will not need again especially old work from past pupils who have now left.
-

Digital Account/Data Retention and Deletion

The following will set out how long we keep files and folders on the network before being deleted, for both staff and pupils.

Pupils

Retention Period: **6 Months**

Pupil accounts are disabled on the day of the final Year 11 exam and archived for approximately 6 months.

All files and folders relating to pupil accounts, including coursework, will be kept for up to 6 months to allow time for ex-pupils to request their personal work or to allow a remark of coursework should evidence be needed.

Staff & Temporary staff

Retention Period: **30 Days**

Staff accounts are suspended at 3:15pm on their final day of contracted work. After this time, access to emails, home area and shared resources will be restricted.

Files and folders in staff home areas will be deleted 30 days after termination of employment date.

Onedrive files will also be kept for 30 days, after this they will be deleted.

Staff should delete all files belonging to themselves before termination of employment.

Staff are permitted to keep files on Departmental Folders/sharepoint after they leave, providing the files will assist Teaching & Learning and be used by current staff.

Emails Retention & Deletion

Emails will be deleted automatically after 15 months (456 Days) from your mailbox for both staff and pupils. This is to reduce the risk of a potential data breach and should be done anyway as ‘good housekeeping’.

Monitoring & Filtering Data

Retention Period: **90 Days**

We will keep records of all activities performed on school systems including webpages accessed, files accessed, keywords and general computer use DFE regulations and the Prevent strategy.

This data may be passed to the headteacher, or relevant authorities should anything suspicious be found.

All data will be kept for 90 days then removed from the system and will only be accessible by the Network Manager.

Physical Data Destruction

- All files and digital data contained on physical, data bearing media, should be destroyed via the correct channels to ensure full compliance with the data protection act.
- All CDs/DVDs/Floppy disks containing data should be passed to the Network Manager for proper disposal and destruction.

- Old USBs containing data may be re-used but must be passed to the Network Manager to be thoroughly wiped and cleaned before re-using.

- All Waste IT Equipment including Computers, Laptops and tablets should be recycled in line with the WEEE directive and data destroyed in line with the Data Protection Act 2018 and Disposal of Assets policy.

- If staff members have any redundant IT equipment containing any data related to work, these should be passed to the Network Manager for secure data destruction this includes personal devices.

- A record of destroyed data will be kept alongside data destruction certificates for as long as the Data Protection Officer deems necessary.

4. Remote Access

For selected staff with Internet access at home, it is possible for them to gain remote access to the school network for the purpose of viewing/editing files. The use of remote access subject to the same rules imposed on staff whilst they are in school and is granted at the discretion of the Network Manager.

Where possible staff should work on files in Onedrive or Sharepoint, which will enable seamless editing of documents without the need to have remote access into the school network.

Access is not a right and may be withdrawn at any time, without prior notice and without reason. Any violation of the terms, as set out may result in the removal of your access outside of school.

Terms of the Agreement

When using any remote access tools staff are bound by the Staff Acceptable Use Agreement alongside the rules below;

The uploading of any files not directly related to your schoolwork is strictly forbidden, as are files of the following nature:

- Any virus infected files;

- Executable files (e.g. computer software, self-extracting archives);

- Command execution files (e.g. JAVA scripts, batch files);

- Files containing any defamatory or unlawful text and/or images;

- Personal music files should not be stored on the system due to copyright issues.

Antivirus

Any computer/terminal you wish to use whilst accessing the school's computer system must have an approved Anti-Virus package installed. If you do not currently have any Anti-Virus software installed, one must be installed before you will be granted remote access. Once installed, the software must be running at all times you are connected/communicating with the school's computer system.

On school provided devices, this will already be installed for you.

You will undertake all reasonable measures to ensure your anti-virus software is kept up to date with the latest software updates and virus detection databases. The following packages are approved:

- Avira Free Antivirus (Free)
- Symantec's Norton Anti-Virus
- Kaspersky
- Panda Free Antivirus
- Windows Defender (Free)

It is possible to view student data remotely via Edulink, including viewing contact details and updating marksheets.

Edulink access must be used by yourself and yourself only. Confidential data can be accessed from within Edulink, and this must be kept private at all times. You must not give your password out to anybody else. It is important to respect and adhere to all Data Protection Laws when accessing sensitive data at home.

Under NO circumstances must you leave your computer/terminal unattended whilst accessing ICT services from outside of school.

By using Remote Access or accessing files/data remotely, you are aware that you are fully responsible for ALL actions carried out in and/or with your account.

Data Protection

Any files containing sensitive information must not be downloaded to any device that is not approved by the IT department, for example you should only access these files on your school laptop, not a personal or borrowed device.

5. Online Safety

Online Safety is a whole school responsibility which encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The headteacher has the right to examine any school owned PCs, laptops, iPads or any other electronic devices and any software or applications held or run on any such devices.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.

- Sound implementation of online safety in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from **Schools Broadband Ltd** including the effective management of **Netsweeper Filter**.
- DFE standards and specifications.

Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

Internet use will enhance learning

- The school internet access is designed expressly for students use and includes filtering appropriate to the age of students.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- Staff and pupils must respect the copyright law 1988.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy as part of the Computing Curriculum.

Managing Internet Access

Information system security

The school's ICT systems capacity and security will be reviewed regularly.

Virus protection will be installed and updated automatically from a dedicated server.

Security strategies will be discussed with the Local Authority.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published unless required by legislation or guidance.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Work can only be published with the permission of the pupils.

Social networking and personal publishing

- School will block access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.
- Pupils should be encouraged to invite known friends only and deny access to others.

Managing filtering & Monitoring

- The school will work in partnership with the internet service provider **Schools Broadband ltd** to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported at once to the Network Manager for screening.
- The use of proxy sites will not be tolerated, and any pupil discovered using these sites will be reported to CL ICT for sanctions to be imposed.
- Senior staff, namely the school DSL will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The DSL will have the responsibility of deciding whether resources should be blocked or allowed, these should be documented in line with KCSIE standards. All requests to allow or block certain resources should be made to the DSL however can be delegated to the Network Manager in clear-cut cases where blocking/allowing resources will be beneficial to teaching & learning while safeguarding staff and pupils.

- Day to day management of Filtering and Monitoring will be undertaken by the Network Manager and IT Support team.

- All computers intended for pupil use will contain remote monitoring software for the purpose of safeguarding.

- Periodic tests will be conducted by the Network Manager and DSL to review the effectiveness of the filtering/monitoring systems.

Managing video conferencing (Teams)

- Video conferencing should use the educational broadband network.
- Pupils should not make or answer a video conference call to an unknown person without staff supervision.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones should not be used in school. The sending of abusive or inappropriate text messages is forbidden.
- The use of mobile phones to take photographs or video footage of incidents i.e. fighting or bullying will not be tolerated.

Protecting personal data

- Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 2018.

Monitoring of network usage

The school reserves the right to monitor and ensure transparency in the use of the school's information systems and Internet access. We may also exercise the right to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place.

Policy Decisions

Authorising Internet access

- All staff must read the full '**Digital Communications Policy**' including the '**Staff Acceptable Use Agreement'** before using any school ICT resource.

- ICT access, including internet access is given at the school's discretion and can be revoked at any time.

- Parents and pupils will be asked to sign and return a consent form when their child enrols at school.

6. Mobile Phone and Personal Devices

A code of conduct is promoted with the aim of creating a cooperative workforce, where staff work as a team, have high values and respect each other; thus, creating a strong morale and sense of commitment leading to increased productivity. Our aim is therefore that all practitioners:-

- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to possible allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Are responsible for self-moderation of their own behaviours.
- Are aware of the importance of reporting concerns promptly It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive.

An agreement of trust is therefore promoted regarding the carrying and use of mobile phones within the setting, which is agreed to by all users.

- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office and/or via landlines or by walkie-talkies where provided. If you are in a location where communication is not possible (e.g. playing fields) and you do not have a walkie-talkie then staff should carry mobile phones for emergency use only.
- Staff should have their phones on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (e.g. classroom, corridor, playground).
- Use of phones (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- Staff must security protect access to their phone.
- Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Headteacher and office staff aware of this, so that messages can be relayed promptly.
- Staff should report any usage of mobile devices that causes them concern to the Headteacher.

- Staff should not use personal mobile devices during Staff Briefings, CPD sessions, meetings or any other professional meetings.

Mobile Phones for work related purposes

We recognise that mobile phones provide a useful means of communication on off-site activities. However, staff should ensure that:-

- Mobile use on these occasions is appropriate and professional.
- Mobile phones should not be used to contact parents during school trips – all relevant communications should be made via the School Mobiles Provided.
- Where possible, staff should not use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras, ipads or school phones. Where this is not possible, photos/videos should be transferred to the school network ASAP and the images deleted off your phone immediately.
- Smart Watches and other wearable devices with the ability to record audio and video, send digital messages and access the internet often mimic the actions of a mobile phone and should be treated as such, adhering to the same rules and code of conduct above.

7. Artificial Intelligence (AI) Policy

Purpose

The purpose of this policy is to outline the appropriate use of Artificial Intelligence (AI) tools within our school to ensure they are used in a responsible, ethical, and secure manner. This policy aims to support staff in leveraging AI for administrative efficiency, enhanced teaching, and improved learning outcomes, while protecting the privacy and security of all stakeholders. It also sets clear guidelines for students on the acceptable use of AI in their academic work.

Scope

This policy applies to all staff, students, and any individuals who have access to the school's IT infrastructure and resources.

Staff Guidelines

1. **Use of AI Tools**
    - Staff are encouraged to use AI tools to assist with administrative tasks, enhance teaching methodologies, and improve learning experiences.
    - The school has access to Copilot by Microsoft (copilot.microsoft.com), which includes commercial-grade data protection. Staff should prioritise using this tool for their AI-related needs.

2. **Data Protection**
    - AI tools provided by the school, such as Copilot, have built-in data protection measures. Personal data, including names and any information that could identify individuals (especially students), should only be entered into these secure tools.
    - Any other AI tool should be treated as a public platform, and staff are prohibited from entering personal data (especially student names or any other sensitive data) into these tools to prevent data breaches and protect privacy.
3. **Accuracy and Reliability**
    - AI tools can sometimes provide incorrect or misleading information. Staff should verify the accuracy of AI-generated content before using it for decision-making or instructional purposes.

Student Guidelines

1. **Use of AI for Academic Work**
    - The use of AI tools to complete homework or assessments is strictly forbidden. Students must produce original work for all assignments and assessments.
    - The school employs AI checkers to ensure the authenticity of student work and to detect any AI-generated content.
2. **Exam Board Guidance**
    - Students must adhere to the guidance provided by exam boards regarding the use of AI. This includes any rules or regulations that may impact their assessments and qualifications.
3. **Permitted Uses of AI**
    - In cases where AI use is permitted, students must seek approval from a teacher and reference the AI tool used in their work.
    - Examples of permitted use may include using AI for research purposes, brainstorming ideas, or as a supplementary tool for learning, provided it is approved by a teacher.
4. **Training and Awareness**
    - Students will receive education on the ethical use of AI, including understanding its limitations, the importance of original work, and the potential consequences of misuse.

General Precautions and Facts about AI

- **Limitations**: AI is not infallible and can produce incorrect or biased information. Users must critically evaluate AI-generated content.
- **Data Privacy**: Protecting personal data is paramount. Only use secure, school-approved AI tools for processing any sensitive information.
- **Ethical Use**: AI should be used to complement and enhance learning and administrative processes, not to replace human judgement or effort.
- **Transparency**: Always disclose the use of AI in any formal or academic work where its use is permitted.

Enforcement

- **Compliance**: All staff and students must comply with this policy. Any breaches will be taken seriously and may result in disciplinary action.

- **Monitoring**: The school will monitor the use of AI tools to ensure compliance and to safeguard the integrity of academic work and data protection.

8. Social Networking

1. PURPOSE

This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of this document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

2. APPLICATION

This applies to all staff employed in delegated schools and those Teachers employed in Centrally Managed Services.

3. BACKGROUND

3.1 The use of social networking sites such as Facebook, Instagram, Snapchat, TikTok and Twitter has over recent years become the primary form of communication between friends and family. In addition, there are many other sites which allow people to publish their own pictures, text and videos such as YouTube, TikTok and Snapchat.

3.2 It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. For example, many schools now use sites such as Facebook and Twitter as a means to enhance parental engagement.

3.3 It is now widely acknowledged that use of such sites does not provide a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees’ consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.

3.4 Difficulties arise when staff utilise these sites and they do not have the relevant knowledge or skills to ensure adequate security and privacy settings. In addition, there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.

4. GUIDANCE AND ADVICE

4.1 Employees who choose to make use of social networking site/media should be advised as follows:-

(i) That they should not access these sites for personal use during working hours.

(ii) That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended; Guidance on Social Media Privacy settings can be obtained from the Network Manager.

(iii) That they do not conduct or portray themselves in a manner which may:-

- bring the school into disrepute.
- lead to valid parental complaints.
- be deemed as derogatory towards the school and/or it's employees.
- be deemed as derogatory towards pupils and/or parents and carers.
- bring into question their appropriateness to work with children and young people.

(iv) That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

(v) On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

*(*In some cases, employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases, employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to this Policy and as such they are potentially placing themselves at risk of formal action being taken under the school's Disciplinary Procedure*.)

4.2 Schools should not access social networking sites in order to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination if for example the selection panel were to discover a candidate held a protective characteristic as defined by the Equality Act.

5. SAFEGUARDING ISSUES

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young people in Educational Settings (May 2019). states:-

12. Communication with children (including the use of technology) In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. Online risks are posed more by behaviours and values than the technology itself.	This means that adults should: ▪ not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used. Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour' Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web-based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable. Staff should, in any communication with children, also follow the guidance in section 7 'Standards of Behaviour'. Staff should adhere to their establishment's policies, including those with regard to communication with parents and carers and the information they share when using the internet. http://www.education.gov.uk/	▪ not give out their personal details ▪ use only equipment and Internet services provided by the school or setting ▪ turn off 3G/4G data access on school premises ▪ follow their school / setting's Acceptable Use Policy ▪ ensure that their use of technologies could not bring their employer into disrepute ▪ not discuss or share data relating to children/ parents / carers in staff social media groups This means that education settings should: • wherever possible, provide school devices such as cameras and mobile phones rather than expecting staff to use their own (e.g. on school trips)