ICT Acceptable Use Policy

Use of computers, network, email, internet, and social media

Date of Last Review:	July 2021
Status:	Non statutory
Governance Lead:	Trust Board
Staff Lead:	Manuela Gordea
Review Process:	Annually
Location:	R:\SLT\Policies
Date of Next Review:	September 2022

1. Introduction

1.1 Those that use the schools' electronic mail services and/or the internet and computers/mobile devices are expected to do so responsibly and to comply with all applicable laws, policies and procedures of the trust and/or its schools, and with normal standards of professional and personal courtesy and conduct.

1.2 E-mail and the internet can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve. The Trust encourages the use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications.

2. Use of School Equipment / Networks

2.1 Computers and laptops, school telephone, mobile phones, other mobile devices loaned to employees by the schools are provided solely to support their professional responsibilities.

2.2 Workers are responsible for the safe and proper use, care and security of equipment and systems provided. Devices must be secured appropriately especially when leaving the school premises (i.e. not left unattended) and protected from unauthorised access or use (i.e. not accessed by family members). Any loss, damage or unauthorised access must be reported immediately.

2.3 Workers must not use school equipment, networks or system to access, download, send or receive, store, create, copy or distribute any material which may be malicious, illegal, libellous, immoral, dangerous or offensive (this includes but is not limited to pornographic, sexual, violent or criminal content and racist, sexist, or otherwise discriminatory material).

2.4 Any appropriate and authorised electronic communication with pupils must be through official school network, channels, and systems and on school equipment.

3. Use of Email

3.1 The email system and the internet/intranet are business tools provided to staff and other users at significant cost. Hence, it is expected that this resource will be used primarily for business related purposes. Reasonable access and use of the internet/intranet and email facilities is also available to recognised representatives of professional associations i.e. Union Officers.

3.2 Trust and schools' businesses must always be conducted through official email addresses, which must be secured with password controls. Workers should respond to emails during working hours in a timely and appropriate fashion.

3.3 Email should be treated like any other form of written communication and, as such, the content should be appropriate and accurate and data protection compliant.

3.4 Extreme care must be taken with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

3.5 Email must not be used to receive, send or forward messages that are defamatory, obscene or otherwise inappropriate. If such an email is received, whether unwittingly or otherwise and from whatever source, this must not be forwarded to any other address and must be reported immediately.

3.6 Electronic media must not be used for knowingly viewing, transmitting, retrieving, or storing any communication that is: discriminatory or harassing, derogatory to any individual or group, obscene or pornographic, defamatory or threatening, illegal or contrary to the trust's policies or business interests.

3.7 All forms of chain mail are unacceptable and the transmission of user names, passwords or other information related to the security of the school's computers is not permitted.

4. Social Networks

4.1 Social networking applications include but are not limited to:

- Trust and Schools websites
- Online discussion forums, for example Facebook;
- Media sharing services for example YouTube;
- Professional networking sites, for example Linked In
- 'Micro-blogging' application for example Twitter

4.2 Where the trust and/or its schools operate official networking sites, these must be managed and used in accordance with this policy. This includes the following requirements:

- use of official (i.e. not personal) email addresses for user accounts;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the schools' logos and other branding elements should be used to indicate the schools support. The schools' logos should not be used on social networking applications which are unrelated to or are not representative of the schools official position;
- users should identify themselves as their official position held within the trust / the schools on social networking applications ;
- any contributions on any social networking application must be professional, uphold the reputation of the schools and be in accordance with data protection requirements;
- users must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religion or other matters;

4.3 Personal use of social media and other on-line applications which may fall into the public domain should not be such that it could bring the school into disrepute and/or call into question an individual's suitability to work with children.

5. Personal use of school Equipment / Networks

5.1 The trust and schools' e-mail, telephones, equipment, systems and internet service may be used for incidental personal purposes, with the approval of the line manager that it does not:

- Interfere with the schools operation of computing facilities or email services.
- Interfere with the user's employment or other obligations to the school.
- Interfere with the performance of professional duties.
- Is of a reasonable duration and frequency.
- Is performed in non-work time.
- Does not over burden the system or create any additional expense to the school.

5.2 Such use must not be for unlawful activities, commercial purposes not under the auspices of the trust and/or its schools, personal financial gain, personal use inconsistent with other trust/schools policies or guidelines, ordering of goods to be delivered to the school address or in the trust/schools name.

5.3 Staff should not store personal photographs using the school network as these are using hard drive space and backup space

5. Security

5.1 The Trust and its schools follows sound professional practices to secure e-mail records, networks, data and system programmes under its control. As with standard paper based mail systems, confidentiality of e-mail cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measures.

5.2 Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered e-mails forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

5.3 In order to effectively manage the security of the email system the following should be adhered to:

- Open mailboxes must not be left unattended.
- Care should be taken about the content of an e-mail as it has the same standing as a memo or letter.
- Report immediately to IT department when a virus is suspected.
- Use appropriate security measures such as encryption/password protection to transmit confidential or sensitive information;
- Ensure all devices and system access are password protected;
- Use secured memory sticks (all laptops, memory sticks and devices used must be encrypted);
- Ensure that pupils are not exposed to any inappropriate images or web links; and

- Respect all copyrights and not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

5.4 Users must not:

- use, transfer or tamper with other people's accounts and files;
- use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use the internet/intranet facilities or equipment to deliberately create any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- monitor or intercept the files or electronic communications of other workers or third parties;
- hack or obtain access to systems or accounts they are not authorised to use;
- use other people's log-ins or passwords; or
- breach, test, or monitor computer or network security measures without authorisation.

5.5 Where any security breach or inappropriate connection or ICT activity occurs, the user must immediately disconnect/log out and report immediately.

6. Privacy and Monitoring

6.1 The Trust and its schools respects users' privacy. Email content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, workers should not have any expectation of absolute privacy in his or her use of the school systems or equipment (including but not limited to networks/servers/internet usage/networks/Wi-Fi). Under the following circumstances such action may be required:

- When required by law.
- If there is a substantiated reason to believe that a breach of the law or trust/schools policies has taken place.
- When there are emergency or compelling circumstances, such as in a disciplinary investigation
- if the school suspects that the employee has been viewing/transmitting offensive or illegal material;
- if the school suspects that the employee has been spending an excessive amount of time on activity which is not work related;
- where required for compliance checks eg auditors, data protection;

6.2 The school reserves the right, at its discretion, to review any employee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other trust or schools policies.

6.3 Employees should not have any expectation of privacy to his or her internet usage. The school will endeavour to notify affected individuals of any monitoring which will take place and the reason for it, what information will be recorded and retained, and for how long, who will have access and how such information will be used, which will include using such information for disciplinary purposes where applicable, save in exceptional circumstances (see below). The school reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors or any other representative of the authorities must be given the right of access to any document, information or explanation that they require.

6.4 Use of the employee's designated personal file area on the network servers provide some level of privacy in that it is not readily accessible by other members of staff.

These file areas may however be monitored to ensure adherence to the Trust's policies and to the law. The employee's personal file area is disk space on the central computer allocated to that particular employee. Because it is not readily accessible to colleagues it should not be used for the storage of documents or other data that should be open and available to others.

6.5 Managers will not routinely have access to an employee's personal file area. However, usage statistics/management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area may be made available.

6.6 Any worker who is unsure about whether or not something he/she proposes to do might breach that policy or if something is not specifically covered in the policy they should seek advice from their line manager or a member of the SLT.

6.7 The school considers the following to be valid reasons for checking an employee's email:

- if the employee is absent for any reason and communications must be checked for the smooth running of the school to continue;
- if the school suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the school understands that it is possible for workers inadvertently to receive such material and they will have the opportunity to explain if this is the case);
- if the school suspects that an employee has been using the email system to send and receive an excessive number of personal communications (or any personal emails if this is prohibited by the school); and if the school suspects that the employee is sending or receiving emails that are detrimental to the school or its pupils.

6.8 The school may monitor communications without notification in certain specific circumstances, including but not limited to;

- establish the existence of facts relevant to the school e.g. whether a contract was entered into by email;
- ascertain compliance with regulatory or self-regulatory practices e.g. checking that the school is complying with external or internal regulations;
- ascertain or demonstrate standards that are or ought to be achieved by workers using the system;
- investigate or detect unauthorised use of the telecommunication system, which would

include checking that workers are not breaching the school's policy on email and internet use; and

- ensure the effective operation of the system, for example through virus monitoring.

7. EMAIL & INTERNET USE AT HOME

7.1 Access to the internet from an employee’s home using a school owned computer/mobile device or through school owned connections must adhere to all the policies that apply to use within the school. Family members or other non-employees must not be allowed to access the schools computer system or use the schools’ computer facilities, without the formal agreement of the Headteacher or CEO.

8. EMAIL PROTOCOLS

8.1 Users must:

- Not ignore e-mails. The system is designed for speedy communication. If the message requires a reply, a response should be sent promptly.
- Not use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details.
- Not abuse others even in response to abuse directed at themselves.
- Not use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
- Not use e-mail, either internally or on the Internet, to sexually harass fellow employees, or harass or threaten anyone in any manner.
- Not use, transfer and tampering with other people’s accounts and files.
- Respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.
- Not use the internet/intranet facilities or equipment to deliberately propagate any virus, worm, “Trojan horse” or any such other programme that is harmful to normal computer operations.
- Not access any obscene or pornographic sites. Sexually explicit or other offensive material may not be viewed, archived, stored, distributed, edited or recorded using the schools networks or computing resources. If a user finds himself/herself connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to the respective line manager or Headteacher. Any failure to report such access may result in disciplinary action.

8.2 Except in cases in which explicit authorisation has been granted by school management, employees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties.

- Hacking or obtaining access to systems or accounts they are not authorised to use.
- Using other people's log-ins or passwords.
- Breaching, testing, or monitoring computer or network security measures.
- E-mail or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else.
- Interfering with other people’s work or computing facilities.
- Sending mass e-mails without consultation with the Headteacher or a senior manager. Global Sends (send to everybody in the Global address book) are not encouraged.
- Using the Internet for personal commercial purposes.

9. DATA PROTECTION (*see also Data Protection Policy)*

9.1 The Data Protection Act 2018 and GDPR regulations 2018 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to e-mail in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights, the trust and its school respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

9.2 As data controller, the schools have responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998 and GDPR 2018.

9.3 In order to comply with its duties under the Human Rights Act 1998, the school is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual’s rights to privacy, taking into account the schools wider business interests. In drawing up and operating this policy the school recognises that the need for any monitoring must be reasonable and proportionate.

9.4 Auditors (internal or external) are able to monitor the use of the schools IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance.

10. EMAIL GOOD PRACTICE GUIDE

	Good Practice
Read Receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the ‘read receipt’ option.
Attachment Formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format

	incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
E-mail Address Groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of e-mails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own e-mail address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential Record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of e-mails could be used in support, or in defence, of the schools legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the e-mail can result in legally binding contracts being put into place.
Distribution Lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them
E-Mail threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already

	exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	E-mail in the right context, care should be taken to use e-mail where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of your email may be interpreted by its recipient.
Forwarding e-mails	Consideration should be given when forwarding e-mails that it may contain information that you should consult with the originator before passing to someone else.
Large E-mails	For larger e-mails, particularly Internet e-mails, where possible send at the end of the day as they may cause queues to form and slow other peoples e-mail.

11. MOBILE PHONES AND OTHER ELECTRONIC DEVICES

11.1 It is accepted that individuals may bring personal mobile phones to school. Personal mobiles should have security codes to prevent access by other persons and must be stored securely and not accessible to pupils at any time.

11.2 Workers are not permitted to use their personal mobile phones to call, text, email or in any other way message pupils/parents/carers. Nor may they divulge their personal telephone number(s) or other contact details to pupils under any circumstances.

11.3 Workers are required to ensure mobile telephones are switched off/to silent during working hours and accessed only during authorised breaks.

11.4 Workers should not bring other electronic devices onto school premises unless this has been specifically authorised by an appropriate manager. In such circumstances, the computer / equipment / mobile device must be kept securely (at the risk of the owner) and security protected so that it cannot be accessed by pupils or others at the school.

11.5 Any personal use of such equipment must be restricted to an employee’s break times or outside their normal working hours and must not impact on their duties in any way.

11.6 Additionally, specific permission must be obtained prior to connecting any device to school networks/systems and the device(s) must have adequate virus protection.

11.7 Workers must ensure that no personal information regarding school business, its pupils or staff is stored on such personal equipment.

11.8 Where exceptionally, specific permission is granted to use personal equipment for work purposes e.g. to give a presentation, the employee must be extremely vigilant that personal files/data etc. are not inadvertently accessed or displayed.

11.9 No pictures or videos may be taken within school or at any school related activity, on personal devises.

12. PERSONAL SOCIAL NETWORKS

12.1 The school recognises individual rights to privacy and a private life. However, the law generally views social media as in the public domain, irrespective of privacy settings. Workers are therefore advised to be mindful of their duties and obligations to uphold the reputation of the school, to comply with the Code of Conduct and other policies and contractual terms in their use of personal social media – being mindful of the real possibility for material to be posted, shared and made public inadvertently or by other contacts.

12.2 The school may require the removal of content it considers inappropriate.

12.3 It is totally unacceptable for any worker to discuss pupils, parents, work colleagues or any other member of the school community or any school related business on any type of social networking site.

12.4 Other posting on personal sites may also impact on the reputation of the school or the suitability/conduct of the employee for example if an employee is off sick but makes comments on a site to the contrary, postings of indecent or inappropriate images/activities etc.

12.5 Workers must not accept or propose contact, nor engage in any conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years.

12.6 Individuals working in the school should not use or access social networking sites of pupils.

Appendix – Agreements re Digital Access

Acceptable Computer and Internet Use Policy

Staff, governors and visitors

The computer system is provided by the Trust and/or its schools and is made available to students, staff, governors and visitors to support and enhance their education, research and work at school. This Policy has been drawn up to protect all parties - the students, the staff and Trust schools.

Staff, governors and visitors must remember that access to the network resources and Internet is a privilege, not a right, and that access requires responsibility.

This policy also applies whenever information is accessed through the schools' remote access, whether or not the computer equipment used is owned by The Trust and/or its schools. The policy applies to all those who make use of school' Service.

- Staff, governors and visitors will only use the schools' email, internet, intranet and any related technologies for professional purposes;
- All Computers or Internet use should be for study purposes, and enhance your work done in the classroom.
- Access should only be made via your authorised username and password which should not be shared; you alone are responsible for your user area. These usernames and passwords should ***never*** be disclosed to anyone.
- The disclosure of private, sensitive, and confidential information should not be allowed through the remote access. Users should not attempt to access the remote access system in any environment where the security of the information contained in the remote access system may be placed at risk e.g. a cybercafé
- Information made available through the remote access system is confidential and protected by law under the Data Protection Act 2018. To that aim: Users must not distribute or disclose any information obtained from the remote access system to any person(s) with the exception of the pupil to which the information relates or to other adults with parental responsibility
- Activity that damages or changes the schools' computer systems, or activity that attacks or corrupts other systems, is forbidden and may be an offence under the Computer Misuse Act 1990;
- Staff, governors and visitors will not install any hardware or software without permission of the Network manager;
- Copyright of materials must be respected; copying of software is not permitted;

- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received; messages should be polite and responsible; only school email will be used;
- Do not reveal personal information, the home address or phone numbers of yourself or other people;
- The use of the computer network for personal financial gain, gambling, political purposes or advertising is forbidden;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- Electronic communications with pupils and staff are compatible with my professional role;
- Staff, governors and visitors should not give out their own personal details such as mobile phone number, personal email address or social network identity to pupils;
- All school ICT equipment should be kept secure, whether in school or off site including travelling from and to work.
- Staff, governors and visitors will only take/store or use pictures of pupils and/or staff only for professional purposes;
- The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Yours sincerely,

A Mohammed CEO

✂……………………………………………………………………………………………

Please print

Staff Name: __________________________(Please Print)

Network Username: __________________________

As a trust/school user of the Internet, I agree to comply with the trust and its schools rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the trust/school.

Staff Signature: ______________________________

Acceptable Computer and Internet Use Policy

Student Version

The computer system is provided by the school and is made available to students and staff to support and enhance their education, research and work at school. This Computer and Internet Use Policy has been drawn up to protect all parties - the students, the staff and the school.

Remember that access to the network resources and Internet is a privilege, not a right, and that access requires responsibility.

Internet access is automatically given to the students when they arrive in school, unless the parents / guardians specifically ask otherwise. This should be in writing.

- All Computer or Internet use should be responsible, sensible and for study purposes, and enhance your work done in the classroom.
- Access should only be made via your authorised username and password which should not be made available to any other person; you alone are responsible for your user area.
- Activity that damages or changes the school computer systems, or activity that attacks or corrupts other systems, is forbidden and may be an offence under the Computer Misuse Act 1990;
- No programs may be brought in on disk or downloaded onto any machine;
- Copyright of materials must be respected; copying of software is not permitted;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received; messages should be polite and responsible;
- Do not reveal personal information, the home address or phone numbers of yourself or other people;
- The use of the computer network for personal financial gain, gambling, political purposes or advertising is forbidden;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
- The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.
- Students will only take/store or use pictures of students and/or staff only for professional purposes.

Sanctions

1. Violation of the above rules will result in a temporary or permanent disabling of Internet and Computer network access.

2. Additional disciplinary action may be added in line with existing school expectations of behaviour.

3. When applicable, outside authorities may be involved.