I have come that they may have life and have it to the full
(John10:10)

ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

This policy is taken from the OLHOC Trust Handbook of Statutory policies and should be read in conjunction with the other policies within the document.

Revised Edition September 2023

ELECTRONIC INFORMATION AND COMMUNICATIONS SYSTEMS POLICY

1. Introduction

1.1. The Trust's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of its provision of excellent service. See also the Trust's Staff Acceptable Use Policy and Monitoring Use of Systems Policy.

1.2. This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff who are required to familiarise themselves and comply with its contents. The Trust reserves the right to amend its content at any time.

1.3. This policy outlines the standards that the Trust requires all users of these systems to observe, the circumstances in which the Trust will monitor use of these systems and the action the Trust will take in respect of any breaches of these standards.

1.4. The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulations together with the Data Protection Act 2018.

1.5. Staff are referred to the Trust's Data Protection Policy for further information. The Trust is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

1.6. All members of staff are required to familiarise themselves with the content of this policy and comply with the provisions set out in it at all times to protect the Trust's electronic systems from unauthorised access or harm.

1.7. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Trust's Disciplinary Policy and Procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

1.8. The Trust has the right to monitor all aspects of its systems, including data which is stored under the Trust's computer systems in compliance with the GDPR and Data Protection Act 2018.

2. Purpose

2.1. The policy has been developed to advise employees of if, when and under what conditions they may use the Trust's communications and information systems for personal reasons. It sets standards to ensure that employees understand the position and do not inadvertently use communications and information in inappropriate circumstances.

2.2. The Trust recognises employees' rights to privacy but needs to balance this with the requirement on the Trust (as a public service) to act appropriately, with probity, to safeguard its business systems, to protect its reputation and to be seen to be doing so.

3. Scope

3.1. This policy covers all forms of communication, information retrieval (from any source), media and equipment, used for official business and regardless of origin, ownership or place of use and the use or misuse of the Trust's equipment or network, for example:

3.1.1. mail systems (internal and external)

3.1.2. internet and intranet (email, web access and video conferencing)

3.1.3. telephones (hard wired and mobile)

3.1.4. fax equipment

3.1.5. computers/laptops/tablet devices – this covers ANY computer or device used for work purposes, whether at the place of work or elsewhere

3.1.6. photocopying, printing and reproduction equipment

3.1.7. recording / playback equipment

3.1.8. video and audio recording including cameras

3.1.9. documents and publications (any type or format)

3.2. The policy applies to all employees, agency staff and to other people acting in a similar capacity to an employee. It will also apply to staff of contractors and other individuals providing services / support to the Trust (e.g. volunteers). It takes account of the requirements and expectations of all relevant legislation.

3.3. Principals / Head Teachers / Managers will discuss the policy with their teams and agree parameters within which team members will act. Every employee will have the policy explained to them at induction. If at any stage employees require further clarification, they should speak to the CEO / Principal / Head Teacher / Manager in the first instance.

3.4. Where an employee needs to discuss personal information with Occupational Health, Personnel or their Trade Union within the workplace, they will be given privacy to do this.

3.5. Principals / Head Teachers / Managers will agree with Trade Union representatives the arrangements for using Trust communication and information systems which will be provided in accordance with any relevant trade union facilities agreement and the ACAS Code of Practice.

4. Equipment Security and Passwords

4.1. All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

4.2. Passwords are unique to each user and must be changed regularly to ensure confidentiality. Staff are required to select a complex password that cannot be easily broken to ensure data and network security. Best practice as recommended by the National Cyber Security Centre is to use three random words.

4.3. Passwords must be kept confidential and must not be made available to anyone except to designated members of IT Support Staff for the purposes of system support..

4.4. Any member of staff who discloses their password to another employee in the absence of express authorisation will be liable to disciplinary action under the Trust's Disciplinary Policy and Procedure.

4.5. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

Commented [JUD1]: Revised to accord with the Staff Acceptable Use Policy

Commented [JUD2]: See above

4.6. If given access to the Trust e-mail system or to the internet, staff are responsible for the security of their terminals / devices. Staff are required to log off or activate a secure password when they are leaving the terminal / device unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team and / or the IT Manager may do spot checks from time to time to ensure compliance with this requirement.

4.7. Staff should be aware that if they fail to log off and leave their terminals/devices unattended they may be held responsible for another user's activities on their terminal/device in breach of this policy, the Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

4.8. Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that they were not the party responsible.

4.9. Staff without authorisation should only be allowed to use terminals / devices under supervision.

4.10. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the CEO / Principal / Head Teacher.

4.11. On the termination of employment for any reason, staff are required to provide details of their passwords and provide a full handover detailing the drives, folders and files where their work can be located and accessed. The Trust reserves the right to require employees to hand over all Trust data held in computer useable format.

4.12. Members of staff who have been issued with a laptop, PDA, tablet, smartphone or other such equipment, must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the device is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

5. Use of Equipment and Materials

5.1. Use of Facilities

5.1.1. The Trust's Code of Conduct that staff must not carry out personal activities during working hours, nor mix private business with official duties.

5.1.2. Official equipment and materials should not be used for general private purposes without prior permission from the CEO / Principal / Head Teacher or an appropriate line manager. This will usually be in writing or may be covered by the parameters agreed by the CEO / Principal / Head Teacher / manager with the team.

5.2. Facilities for Private Use

5.2.1. If an employee needs to use a Trust phone (e.g. at their desk) for private purposes that are permissible within this policy, the call should be timed, and the payment made to the office. Payment is not required where employees need to phone to notify someone they have been delayed at work or in other emergencies.

5.2.2. In terms of using other equipment and materials belonging to the Trust, the decision to allow such use is at the Principal's / Head Teacher's / Manager's discretion. However, the following are provided as examples to illustrate where it might be reasonable for permission to be given for reasonable use for private purposes, under the conditions shown and after getting prior approval, in writing if this is required. The CEO / Principal / Head Teacher or a senior manager may veto private use at any time if they consider that circumstances justify this in general or particular cases, e.g. because of improper use or over-use. A charge may be made for materials if the values are significant.

5.2.3. Social or recreational activities associated with Trust employment.

5.2.4. Regular activity for a legitimate voluntary body or charity – but prior written approval from a senior manager must be obtained.

5.2.5. Training or development associated with Trust employment.

5.2.6. Occasional and brief essential family communications or other personal messages. In emergencies permission might need to be obtained retrospectively or again this may be covered by the general parameters agreed with the team.

5.2.7. If given permission, approved acceptable private use should normally take place in the employee's own time but where this is not practicable or sensible, any disruption to the employee's official work or that of colleagues must be minimal. Official work will always take precedence.

5.3. All uses, whether for private or official purposes, must observe:

5.3.1. The law.

5.3.2. The Trusts' relevant policies and procedures (e.g. Social Media Policy, Data Protection Policy etc.)

5.3.3. Academy Trust Handbook

5.3.4. All terms of employment, especially the Code of Conduct for Employees.

5.3.5. The specific points in 5.4 below

5.4. It is not acceptable to use Trust equipment and materials or an employee's own equipment / materials in the workplace in any of the following contexts:

5.4.1. Illegal activity.

5.4.2. Activities for private gain.

5.4.3. Personal shopping.

5.4.4. Excessive personal messages.

5.4.5. Playing games.

5.4.6. Gambling.

5.4.7. Political comment or any campaigning.

5.4.8. Personal communications to the media.

5.4.9. Use of words or visual images that are offensive, distasteful or sexually explicit.

5.4.10. Insulting, offensive malicious or defamatory messages or behaviour.

5.4.11. Harassment or bullying.

5.4.12. Random searching of the web.

5.4.13. Accessing sites which could be regarded as sexually explicit pornographic or otherwise distasteful or offensive.

5.4.14. Using message encryption or anonymised web search, except where encryption is required for official Trust business purposes.

5.4.15. Racist, sexist or other conduct or messages which contravene the Trust's employment diversity policies.

5.4.16. Actions which could embarrass the Trust or bring it into disrepute.

6. Systems Use and Data Security

6.1. Members of staff must not delete, destroy or modify any of the Trust's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the Trust, its staff, students, or any other party.

6.2. All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the IT Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

6.3. Where consent is given all files and data should always be virus checked before they are downloaded onto the Trust's systems. If in doubt, the employee should seek advice from the Director of E-Systems or a member of the Senior Leadership Team.

6.4. The following must never be accessed from the network without prior authorisation from the IT Department / Head Teacher, because of their potential to overload the system or to introduce viruses:

6.4.1. audio and video streaming;

6.4.2. instant messaging;

6.4.3. chat rooms;

6.4.4. social networking sites;

6.4.5. web mail (such as Hotmail or Yahoo) and

6.4.6. WhatsApp.

6.5. No device or equipment should be attached to the Trust's systems without the prior approval of the IT Manager or Senior Leadership Team. This includes, but is not limited to, any PDA or tablet, telephone, USB device, iPod, digital camera, MP3 player, infra-red or wireless connection device or any other device.

6.6. The IT Manager should be informed immediately if a suspected virus is received. The Trust reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The Trust also reserves the right not to transmit any e-mail message.

6.7. Staff must not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

6.8. Misuse of the Trust's computer systems may result in disciplinary action up to and including summary dismissal.

6.9. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the Trust's Systems and guidance under "E-mail etiquette and content" below.

7. E-mail Etiquette and Content

7.1. E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

7.2. The Trust's e-mail facility is intended to promote effective communication within the business on matters relating to the Trust's business activities and access to the Trust's e-mail facility is provided for work purposes only.

7.3. Staff are permitted to make occasional personal use of the Trust's e-mail facility provided such use is in strict accordance with this policy (see Personal Use below). Excessive or inappropriate personal use of the Trust's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

7.4. Staff should always consider if e-mail is the appropriate medium for a particular communication. The Trust encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

7.5. Messages sent on the e-mail system should be written as professionally as a letter and should be concise and directed only to relevant individuals on a need-to-know basis. The content and language used in the message must be consistent with the Trust's best practice.

7.6. E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft e-mail first, print it out and review it carefully before finalising and sending. Hard copies of e-mails should be retained on the appropriate file.

Commented [ELA3]: This sentence can be deleted if it does not accord with current practice

7.7. All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc. against both the member of staff who sent them and the Trust. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the Trust in the same way as the contents of letters or faxes.

7.8. E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated, and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

7.9. Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The Trust's standard disclaimer should always be used on every e-mail.

7.10. Staff should ensure that they access their e-mails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to e-mails marked 'high priority' as soon as is reasonably practicable.

7.11. Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately.

7.12. If a recipient asks you to stop sending them personal messages, then always stop immediately. Where appropriate, the sender of the e-mail should be referred to this policy and asked to stop sending such material.

7.13. If you feel that you have been harassed or bullied or are offended by material sent to you by a colleague via e-mail, you should inform the CEO / Principal / Head Teacher who will usually seek to resolve the matter informally. You should refer to the Trust's Equal Opportunities Policy and the Harassment and Bullying Policy for further information and guidance.

7.14. If an informal procedure is unsuccessful, you may pursue the matter formally under the Trust's formal grievance procedure. (Further information is contained in the Trust's Equal Opportunities Policy, Harassment and Bullying Policy and Grievance Policy and Procedure set out in this handbook).

8. As General Guidance, Staff Must Not:

8.1. Send or forward any e-mail containing swear words or that may be considered offensive or abusive.

8.2. Send any e-mail or attachments, including resending and forwarding, which may be regarded as harassing or insulting or of a pornographic, illegal, violent, sexist, or racist nature or that may be constructed as libellous;

8.3. Send e-mails or attachments which contain copyright material to which the Trust does not have distribution rights is not permitted.

8.4. Use personal e-mail addresses by Staff for any official Trust business;

8.5. Send or forward private e-mails at work which they would not want a third party to read.

8.6. Send or forward chain mail, junk mail or trivial messages etc which may contribute to system congestion. Spam or junk mail will be blocked and reported to the e-mail provider;

8.7. Send any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) or is confidential in nature. Such e-mails will only be sent using secure and encrypted e-mail or password protection. Sending such e-mails by unsecure means is prohibited.

8.8. Send e-mails containing children's full names either in the subject line or in the main body of the text. Initials should be used wherever possible.

8.9. Attempt to access Trust /setting e-mail systems. Such access will always take place in accordance with data protection legislation and in line with other appropriate Trust/setting policies e.g. confidentiality.

8.10. Use Trust -email addresses and other official contact details for setting up personal social media accounts.

8.11. Send e-mail which contain personal opinions about other individuals, e.g. about Staff, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

8.12. Send e-mails selling or advertising goods or services or broadcasting messages about sponsorship or charitable appeals or lost property, as other more appropriate forums are available for these purposes.

8.13. Agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained.

8.14. Send e-mails from another worker’s computer under an assumed name unless written authorisation has been granted.

Commented [JUD4]: These accord with the Staff Acceptable Use Policy where appropriate

8.15. With regards to Paragraphs 8.1 to 8.14, please also see the Trust’s Staff Acceptable Use Policy.

8.16. E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service-related issues. Urgent or important messages to family and friends are permitted but must be of a serious nature.

8.17. The Trust recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

8.18. Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way. The CEO / Principal / Head Teacher should be informed as soon as reasonably practicable.

9. Inadvertent Access to Inappropriate Sites and Inappropriate Emails

9.1. If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify their line manager of the incident, giving the date and time, web address (or general description) of site and the action taken. This will help safeguard their position in circumstances where disciplinary action would otherwise result.

9.2. Employees may find themselves receiving emails which contravene this policy. In the case of comparatively innocuous material (e.g. 'clean jokes'), the recipient should point out to the sender that they do not wish to receive such messages at their workplace because they believe they contravene the Trust’s policy. If there is repetition, the employee should retain the messages and notify their line manager. If the emails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the CEO / Principal / Head Teacher notified immediately. Employees should notify the sender that they do not wish to receive further such material and keep a record of doing so.

10. Use of the Internet

10.1. When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the Trust, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

10.2. Staff must not access any web page or any files from the Trust’s systems (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

10.3. As a general rule, if any person within the Trust (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the Trust's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

10.4. Staff should not under any circumstances use the Trust's systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

10.5. Staff are reminded that text, music and other content on the internet may be copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

10.6. The Trust's website is intended to convey its core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Team in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

10.7. Staff are not permitted to use WhatsApp for any Trust related matter and should refrain from texting and using personal phones. The Trust requires its staff to speak to colleagues directly or use alternative systems to make contact with staff (such as e-mails).

11. Inappropriate Use of Equipment and Systems

11.1. Occasional personal use is permissible provided it is in full compliance with the Trust's rules, policies and procedures (including this policy, the Equal Opportunities Policy, Harassment Policy, Data Protection Policy, Code of Conduct and Disciplinary Policy and Procedure).

11.2. Misuse or abuse of the Trust's telephone or e-mail systems or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the Trust's Disciplinary Policy and Procedure.

11.3. Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

11.3.1. accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;

11.3.2. transmitting a false and/or defamatory statement about any person or organisation;

11.3.3. sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;

11.3.4. transmitting confidential information about the Trust and any of its staff, students or associated third parties;

11.3.5. transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Trust;

11.3.6. downloading or disseminating material in breach of copyright;

11.3.7. copying, downloading, storing or running any software without the express prior authorisation of the IT Manager;

11.3.8. engaging in online chat rooms, instant messaging, social networking sites and online gambling;

11.3.9. forwarding electronic chain letters and other materials;

11.3.10. accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child;

11.3.11. accessing sites promoting radicalisation, terrorism etc.

Commented [JUD5]: Added to accord with the Staff Acceptable Use Policy

11.4. Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

11.5. Where evidence of misuse is found the Trust may undertake a more detailed investigation in accordance with its Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary process.

11.6. If necessary, such information may be handed to the police in connection with a criminal investigation.

12. Monitoring

12.1. The content of the Trust's IT resources and communications systems are the Trust's property.

12.2. The Trust's systems provide the ability to monitor telephone, e-mail, voicemail, internet and other communications traffic. For business reasons and to perform its various legal obligations in connection with its role as an employer, the Trust's systems including the telephone and computer systems, and any personal use of them, is electronically monitored from time to time.

12.3. Staff should have no expectation of privacy in any message, file, data, document, facsimilie, telephone conversation, social media post conversation or message, or any other kind of information or communication transmitted to, received or printed from, or stored or recorded on the Trust's electronic information and communication systems.

12.4. The Trust reserves the right to monitor, intercept and review, without further notice, staff activities using its IT resources and communications systems, including but not limited to social media postings and activities, to ensure that its rules are being complied with and for legitimate business purposes. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, logins, recordings and other uses of the system as well as keystroke capturing and other network monitoring technologies.

12.5. The Trust may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

12.6. Monitoring will only be carried out the extent permitted or required by law and as necessary and justifiable for business purposes. Information obtained through monitoring will not be accessible (or distributed) any more widely than is necessary for the purposes for which it was gathered.

12.7. Staff are advised not to use the Trust's IT resources or communications systems for any matter they wish to be kept private and confidential.

12.8. All employees should be made aware at induction, at intervals thereafter and possibly through automatic messages on Trust equipment, that, in relation to any electronic communication, there can be no expectation of absolute privacy when using Trust equipment provided for official / work purposes; and that the Trust reserves the right to monitor all communications including their content.

12.9. The Trust may undertake monitoring to ensure that equipment and systems are used efficiently and effectively and that the use of e-mail or the internet is legitimate and in accordance with this policy; to find lost messages or to retrieve messages or data lost due to computer failure; to maintain systems security; to assist in the investigation of wrongful acts and/or to comply with any legal obligation. Normally monitoring consists of the following:

12.9.1. **Telephones and fax**. The Trust reserves the right to monitor communication content selectively if abuse is suggested. However, such monitoring would only take place following an assessment that such steps are necessary to further a particular investigation or concern. Where calls are made via the Trust network, an automatic record is kept of every number called, from where and the duration of the call. Further action is taken where particular numbers called or the frequency and duration of calls suggest abuse of this policy. Telephone response times will be sampled from time to time.

12.9.2. **Emails**. When using the Trust e-mail system every incoming and outgoing email message is automatically swept for key words, attachments, viruses and spam which could indicate misuse or a threat to the rest of the network.

12.9.3. **Web access**. When using the Trust internet, access to some web sites is automatically prevented (e.g. pornographic, racist, social media and violent sites). An automatic record is made of all sites visited and a sweep made of site names and content against pre-determined criteria, to identify inappropriate sites together with attempts made to access such sites. The Trust reserves the right to apply similar restrictions and screening to its own web access systems.

12.9.4. **PC's** – Monitoring software is installed on all PC's and the Trust's remote access, which logs all user activity throughout the day on the Trust network. This information can only be accessed by the Trust's Information & Communication Technology Services team and auditors unless the Principal /Head Teacher/Senior Manager suspects misuse and then access will be given. The Trust reserves the right to spot check logs.

Commented [ELA6]: Update if the team has a different name

12.9.5. **Mail**. The privacy of internal and external postal communications marked 'personal' will normally be respected (unless abuse of this policy is suspected) but all other communications may be opened for good reason on authorisation by a CEO / Principal / Head Teacher or member of the Senior Leadership Team.

13. Access to and Retention of Monitoring Information

13.1. Access to routine monitoring information is restricted to specified employees in Information & Communication Technology Services and Audit. If they identify a potential issue of abuse the relevant CEO / Principal / Head Teacher / Senior Manager will be given access to the information to enable appropriate action to be taken. They will respect the confidentiality of all communications and disclose the contents of communications only where there are grounds for suspecting abuse of this policy. Where this is the case, other Senior Managers may then be involved and are likely to be made aware of the contents of communications.

Commented [ELA7]: Update if the team has a different name

14. Surveillance

14.1. Permanently fitted surveillance cameras are installed by individual schools, where applicable, for the prevention and detection of crime, security, protection of students and staff and health and safety reasons and will always be visible to people within their range. There are strict controls over this recorded data and under normal circumstances no such data will be retained for longer than [7] days. Any questions about data held in this way should be addressed to the CEO / Principal / Head Teacher in the first instance. Video recording tapes will be kept secure and no automatic connections will be made between information from security cameras and other monitoring sources.

Commented [ELA8]: This information should be included in a monitoring policy

14.2. Covert monitoring will only be used in connection with a criminal investigation or where abuse of terms of employment, e.g. the sickness scheme, is being investigated. This will always be in accordance with the statutory safeguards applicable to such activity (the Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998) and only authorised following careful consideration of the need for such action in accordance with the Regulation of Investigatory Powers Act 2000.

14.3. This policy provides safeguards in relation to whom can sanction covert surveillance, the reasons it can be undertaken and how long it can continue.

15. Security

15.1. Every employee must observe the Trust's communications and information technology security requirements (as detailed in the Staff Acceptable Use Policy) and act responsibly when using equipment and materials.

15.2. Employees will be provided with the necessary briefing and training to enable them to comply with this requirement. The CEO / Principal / Head Teacher will take the most serious view of any action or inaction on the part of an employee who deliberately, recklessly or carelessly jeopardises the security of records or systems.

15.3. Any employee detecting a potential security problem (e.g. a virus or unauthorised access) must immediately take any action within their authorised power to safeguard or resolve the situation (e.g. disconnect any infected device from the network (remove the cable) and, if appropriate, notify the person responsible for ICT) and notify the CEO / Principal / Head Teacher or a Senior Manager.

16. Reporting Misuse

16.1. If any employee suspects activity which may constitute misuse or activities which could jeopardise system security, they must report this immediately to the CEO / Principal / Head Teacher or a Senior Manager. The CEO / Principal / Head Teacher or a Senior Manager must consider whether it would be appropriate to involve Internal Audit (Dains) and must always ensure that all relevant records and documents (paper and electronic) are safeguarded and retained securely. If necessary, a strategy for investigation will be agreed between the CEO / Principal / Head Teacher / Manager who will take legal advice as necessary.

Commented [ELA9]: Revise as applicable if the Trust does not have such a team

17. Consequences of Breach: Disciplinary Action

17.1. Breaches of this policy may result in the application of the Disciplinary Policy and Procedure and may, if deemed sufficiently serious, be treated as gross misconduct.

17.2. In the case of contractors, agency staff, volunteers or partnership employees, breach may result in termination of the contract or relevant arrangement and/or withdrawal of the relevant facility.

17.3. Police involvement and prosecution may follow if the conduct in question constitutes possible criminal activity.

18. Use of Laptops / Tablets Outside the Trust

18.1. Laptop computers and / or tablets are supplied to ***facilitate the flexible use of the equipment both at home or at work***.

18.2. Academies nominate named teachers to receive the equipment.

18.3. Ownership will remain with the Trust and the teacher will be required to return the equipment if employment at the Trust ceases.

18.4. Any laptop computer and / or tablet provided to a teacher will be made available on a long-term loan basis for ***their professional use only***. ***It is expected that this will include use at various locations including the teacher's home and at work.*** However, no expectation may be placed on the teacher to make the laptop / tablet available for regular use at work as part of the Trust's general ICT provision.

18.5. The Trust would like to draw staff attention to:

18.5.1. The dangers of virus infection

18.5.2. The Data Protection Act 2018: The Act requires, amongst other things, that all personal data should be protected by appropriate security safeguards against unauthorised use or unlawful processing of personal data and against accidental loss or destruction or damage.

18.5.3. Copyright, Design and Patents Act 1988: All software must be used only in accordance with the terms of the licence. Generally, the making of copies is forbidden and is a criminal offence.

18.5.4. Computer misuse Act 1989: Identifies three main offences concerning unauthorised access to system, software or data. The punishment depends upon whether the intent of the hacker was merely to gain access, to commit further offences after gaining access or to make a modification to 'computer material' e.g. inject a virus.

18.5.5. Trust policies on the inappropriate use of computers.

18.5.6. Health and Safety issues.

19. The Trust has clearly established policies and practices guiding the use of computer and other equipment within its communications and information acceptable use policy.