Treetops Learning Community

E-Safety Policy

December 2021

Treetops Learning Community

E-Safety Policy

Document Detail	
Authorised By:	Trustees
Date Approved:	December 2021
Next Review Date:	Ratified by Trustees at the December Board meeting each year

Contents

This policy sets out the TREETOPS SCHOOLS expectations of staff/pupils and other users (working for or on behalf of the school), in respect to the use of all electronic communication via the schools internet activity or computer equipment. This policy applies to all electronic mail systems, video conferencing equipment and any other services provided by the school, all users and holders of the schools e-mail and internet services.

This policy is designed to express the school's philosophy with regard to electronic communication and to set forth general principles employees and pupils should apply when using electronic media and service. This guidance does not attempt to cover every possible situation, but has been compiled having consulted **Education for a Connected World – 2020 edition**
UK Council for Internet Safety. (see Appendix 3)

1. Introduction

Electronic communication 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 school encourages the use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications including the safe provision for students online as recommended by the Department for Education. (see Appendix 4)

2. Objectives

The objective of this policy is to ensure that:

- The school community is informed about the applicability of policies and laws to e-safety.
- Electronic mail services and the internet are used incompliance with those policies and laws.
- Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and
- Disruptions to the school's electronic mail and other services and activities are minimized.

3. Usage

Those that use the school's electronic communication systems are expected to do so responsibly, comply with all applicable laws, other policies and procedures of the school, and with normal standards of professional and personal courtesy and conduct. Appendix 1 provides an illustration of good e-mail practice.

4. Security

The school follows sound professional practices to secure e-mail records, 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 measure.

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.

In order to effectively manage the e-mail system, the following should be adhered to:

- Open mailboxes must not be left unattended
- Care should be taken about the content of an e-mails it has the same standing as a memo or letter. Both the individual who sent the message and/or the school can be sued for libel.
- Reporting immediately to ICT Units when a virus is suspected in an e-mail

5. Misuse & Prohibited Communications

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
- Engaged in any purpose that is illegal or contrary to the school's policy or business interests.

Further, 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. 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.
- Using electronic media and services must not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
- Anyone obtaining electronic access to other companies' or individuals' material must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Law and school policy prohibit the theft or abuse of computing resources. This applies to e-mail and internet services and includes:

- Unauthorised entry.
- Use, transfer and tampering with other people's accounts and files.
- Interfering with other people's work or computing facilities.
- Sending, storing or printing offensive or obscene material including content that may be interpreted as sexual or racial harassment.
- Mass mailing or personal messages.
- Internet use for personal commercial purposes.

- Using 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.
- Assessing any obscene or pornographic sites. Sexually explicit material may not be viewed, archived stored, distributed, edited or recorded using the school's 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 tot eh respective line manager or Headteacher. Any failure to report such access may result in disciplinary action.

It is impossible to define all possible unauthorised use, however, disciplinary action may be taken where an employee's actions warrants it. Other actions deemed unacceptable, although not exhaustive, include:

- Theft or copying of files without permission.
- Sending or posting the schools or local authorities confidential files outside of the organisation or inside the organisation to unauthorised staff.
- Refusing to co-operate with reasonable security investigation.

6. Personal Use

The electronic communication systems 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. Reasonable access and use of the electronic communication system facilities is also available to recognise representatives of professional associations, i.e. Union Officers.

The schools e-mail and internet service may be used for incidental personal purposed, with the approval of the Headteacher, provided it does not:

- Interfere with the school's operation of computing facilities or e-mail 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.

Such use must not be for:

- Unlawful activities.
- Commercial purposes not under the auspices of the school.
- Personal financial gain.
- Personal use inconsistent with other school policies or guidelines.

All such use should be done in a manner that does not negatively affect the use of the school's systems for business purposed. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

7. Privacy

The school respects user' privacy. E-mail content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- When required by the law.
- If there is a substantiated reason to believe that a breach of the law or school policy has taken place.
- When there is an emergency or under compelling circumstances.

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 school policies.

Employees should not have any expectation of privacy to his or her internet usage. 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 must be given the right of access to any document, information or explanation that they require.
Use of employee's designated personal file area[1] on the network server provides some level of privacy in that it is not readily accessible by other members of staff. These file areas will however be monitored to ensure adherence to the school'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 in the office.

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 are will be made available from time to time.

8. E-mail & Internet use at home

Access to the internet from an employee's home using a school owned computer or through 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 school's computer system or use the schools computer facilities, without the formal agreement of the Headteacher.

Pupils will be encouraged to use the internet responsibly at home and school via termly e-safety lessons.

9. Policy Violations

Staff who abuse the privilege of school-facilities access to electronic media or services face being subjected to disciplinary action, up to and including termination of employment, and risk having the privilege removed for themselves and possibly other employees.

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.

- 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.
- Abuse others (known as 'flaming'), even in response to abuse directed at themselves.

[1] Everyone has the right to respect for his private and family life, his home and his correspondence.

- Use e-mail, either internally or on the Internet, sexually harass fellow employees, or harass or threaten anyone in any manner.
- Send e-mails to more than 100 recipients without consultation with the Headteacher. Global Sends (end to everybody in the Global address book) are prohibited.

Before storing confidential information in this way, employees are advised to ensure that they understand how to save information to their personal file area.

10. Protection

The Data Protection Act 1998 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[2], the school respects the right to privacy for employees who use ICT equipment but does not offer any guarantee of privacy to employees using ICT equipment for private purposed.

As data controller, the school has responsibility for any data processed or stores 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.

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.

Auditors (internal and external) are able to monitor the use of the school's ICT 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 practices 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[3]. (See Appendix 2)

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

3. Directed Surveillance' is defined as surveillance which is covert (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place) but not intrusive, for the purpose of a specific investigation in such a manner as is likely to result in the obtaining of private information about a person.

Appendix 1

E-Mail 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 the most important, or to spot on they are waiting for.
Subject	Avoid sending messages dealing wit 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 archive.
Recipients	Beware of ending 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 of who have central interest. Cc to indicate those who have peripheral interest and who 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 to forget that electronic conversions 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-mail could be used in support, or in defence, of the schools legal position in the even 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 tat 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 e-mail 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.

Appendix 2

Legislative Framework

The Human Rights Act 1998

This provides for the concept of privacy giving a 'right to respect for private and family life, home and correspondence'. The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act. Halford v UK 1997 suggest that employees have reasonable expectations of privacy it eh workplace, and employers are recommended to provide workers with some means of making personal communications which are not subject to monitoring, for instance a staff telephone line or a system of sending private e-mails which will not be monitored.

Convert monitoring is likely to be unlawful unless undertaken for specific reasons as set out in the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception o Communications) regulations 2000 (see below). Employers should make sure workers know of any monitoring or recording of correspondence (which includes e-mails, use of Internet, telephone calls, faxes and so on).

Regulation of investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system, and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer f or the unlawful interception of communications.

There are two areas where monitoring is not unlawful. These are:

- where the employer reasonably believes that the sender and intended recipient have consented to the interception.

- Without consent, the employer may monitor in the following circumstances, as set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. these include:

- to ensure compliance with regulatory practices e.g. Financial Services Authority requirements
- to ensure standards of service are maintained, e.g. in call centres
- to prevent of detect crime
- to protect the communications system, this includes unauthorised use and potential viruses
- to determine the relevance of the communication to the employer's business, i.e. picking up relevant messages when someone is away from work.

However, the employer is expected to make all reasonable efforts to ensure system users know that communications may be interpreted, and any such monitoring must also comply with the provisions of the Data Protection Act 1998 (see below), and in particular the Data Protection principles on fair processing.

Data Protection Act

The Information Commissioner – responsible for enforcement of the Data Protection Act – is publishing four codes of practice to help employers comply with the provisions of the Data Protection act. These codes clarify the Act in relation to processing on individual data, and the basis for monitoring and retention of e-mail communications.

The code of practice *Monitoring at work: an employer's guide* states that any monitoring of e-mails should only be undertaken where:

- the advantage to the business outweighs the intrusion into the workers' affairs
- employers carry out an impact assessment of the risk they are trying to avert, workers are told they are being monitored
- information discovered through monitoring is only used for the purpose for which the monitoring was carried out
- the information discovered is kept secure
- employers are careful when monitoring personal communications such as e-mails which are clearly personal
- employers only undertake convert monitoring in the rarest circumstances where it is used for the prevention or detection of crime.

Telecommunications (Lawful Business Practice) (Interception of Communications Regulations 2000

This Act empowered the Secretary of State to make regulations, which allow businesses to intercept communications in the course of lawful business practice and in specific circumstances without eh express consent of either the sender or the recipient. Under the regulations, businesses are required to make all reasonable efforts to inform users of their own systems that such interceptions might take place.

Contract Law

It is just as possible to make a legally binding contract via e-mail as it is by letter or orally. Workers need to be aware of the danger of inadvertently making contracts on behalf of their employer, or varying the terms off any existing contract.

Copyright Law

The copyright, designs and Patents act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly copyright exists over software, which should not be downloaded without licence.

Obscene Publications Act 1959, Protection so Children act 1988, criminal Justice act 1988

These acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace the downloading of certain images from the Internet might subject a worker to charges of criminal behaviour.

Computer Misuse act 1990

This Act is mainly concerned with the problems of 'hacking into computer systems.

Lawful Business Practice Regulations (LBP)

The LBP Regulations authorise employers to monitor or record communications without consent for a number of purposes, including the following:

- To establish the existence of facts relevant to the business.
- To ascertain compliance with the regulatory or self regulatory practices or procedures relevant to the business.
- To ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.
- To prevent or detect crime.
- To investigate or detect the unauthorised use of telecommunications including those that are Internet Based, by fax and by e-mail.

Appendix 3

Education for a Connected World – 2020 edition
UK Council for Internet Safety

Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.

Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.

Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.

Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.

Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.

Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.

Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.

Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

Appendix 4

Teaching online safety in school
Department for Education – June 2019

Summary

1. This is non-statutory guidance from the Department for Education.

2. It outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements. It complements existing and forthcoming subjects including Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing. It does not imply additional content or teaching requirements.

Expiry or review date

3. This guidance will be reviewed before September 2020.

Who is this publication for?

4. This guidance is for school leaders, school staff and governing bodies. It applies to all local authority maintained schools, academies and free schools.

5. The interventions and support information may also be helpful for early years settings, colleges and other post-16 institutions.

Main points

6. It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app (page 6).

7. However, schools also need an understanding of the risks that exist online so they can tailor their teaching and support to the specific needs of their pupils (page 8).

8. Schools can refer to the Education for a Connected World Framework for age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

9. When planning their curriculum, and how online safety fits within it, there are a number of areas we recommend schools consider, for example how to support vulnerable pupils (page 24).

10. We recommend that schools embed teaching about online safety and harms within a whole school approach (page 26).

Introduction

11. Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks.

12. We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

13. This advice brings together information that will help schools deliver online safety content within their curriculum and embed this within their wider whole school approach.