




Trafford Alternative Education Provision

E - SAFETY AND DATA SECURITY POLICY

[2020]

Policy Name:	E - Safety and Data Security Policy
Policy Number:	3
Date of Approval:	December 2020
Review Date:	December 2022
Person Responsible:	Lynda Thompson Executive Headteacher
Approved By:	Lynda Thompson Executive Headteacher
For Action By	Senior Leadership Team
For Information to:	Teaching Staff/ Parent/Carer(s) Students
General Data Protection Regulations (GDPR)	<p>This policy document has been reviewed in compliance with GDPR (May 2018)</p> <p>Lynda H Thompson, Executive Headteacher</p> 

Trafford Alternative Education Provision

Our Mission Statement:

Trafford Alternative Education Provision is committed to providing...

A 21st Century education that promotes the academic, emotional and social development of our students. Our aim is to create a holistic, nurturing and inspiring environment where students are supported and encouraged to take charge of their lives, their learning and their decisions. Every student will have an understanding of their personal journey, challenges and future opportunities. All will be encouraged to become independent thinkers and learn to value and respect others thus enabling them to meet the challenges of the wider world. In partnership with parents, carers, schools and outside agencies we will provide students and staff with a positive and supportive learning experience.

We will achieve our vision by constantly thinking about the bigger picture, working as one team, valuing our staff and their continual development and by frequently reviewing, debating and developing the curriculum.

Contents

1. Introduction
2. Managing Other Online Technologies
3. Monitoring
4. Breaches
5. Incident Reporting
6. Equal Opportunities
7. Staff Usage
8. Removable Media
9. E-Safety – Roles and Responsibilities
10. E-Safety in the Curriculum
11. Incident Reporting, E-safety Incident Log & Infringements
12. Misuse and Infringements
13. Storage of Images
14. Personal Mobile Devices (including phones
15. ICT Systems
16. Use of the Internet
17. Unacceptable Usage of ICT, Internet and Email facilities
18. How to Make a Complaint

1. Introduction

1.1 Information and Communications Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Trafford Alternative Education Provision needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

1.2 ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

1.3 Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

1.4 At Trafford Alternative Education, we understand the responsibility to educate our students on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

1.5 Trafford Alternative Education holds personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the Trafford Alternative Education Provision. This can make it more difficult for your Trafford Alternative Education Provision to use technology to benefit learners.

1.6 Everybody in the Trafford Alternative Education community has a shared responsibility to secure any sensitive information used in their day to day

professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

1.7 This policy and the Acceptable Use Agreement for students are inclusive of both fixed and mobile internet; technologies provided by the Trafford Alternative Education Provision (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

1.8 Trafford Alternative Education Provision via Trafford IT also employs some additional web-filtering which is the responsibility of an SLA with Trafford IT Department.

1.9 Trafford Alternative Education Provision is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998. Staff and students are aware that Trafford Alternative Education Provision based email and internet activity can be monitored and explored further if required

1.10 Trafford Alternative Education does not allow students access to internet logs. It uses management control tools for controlling and monitoring workstations

1.11 If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

1.12 It is the responsibility of Trafford Alternative Education Provision, by delegation to the network manager (Trafford IT) to ensure that anti-virus protection is installed and kept up-to-date on all Trafford Alternative Education Provision machines.

1.13 Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the Trafford Alternative Education Provision's responsibility nor the network managers to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the (*technician/teacher*) for a safety check first.

1.14 Students and staff are not permitted to download programs or files on Trafford Alternative Education Provision based technologies without seeking prior permission from the Executive Headteacher.

1.15 If there are any issues related to viruses or anti-virus software, the network manager should be informed by email to Trafford IT.

2. Managing Other Online Technologies

2.1 Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

2.3 At present, the Trafford Alternative Education Provision endeavors to deny access to social networking and online games websites to students within Trafford Alternative Education Provision.

2.4 All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are

2.5 Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

2.6 Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, Trafford Alternative Education Provision details, IM/ email address, specific hobbies/ interests). Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals. Students are also encouraged to be wary about publishing specific and detailed private thoughts and information online. All students are asked to report any incidents of Cyberbullying to the Trafford Alternative Education Provision.

3. Monitoring

3.1 Authorised ICT staff may inspect any ICT equipment owned or leased by the Trafford Alternative Education Provision at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

3.2 ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Trafford Alternative Education Provision business related information; to confirm or investigate compliance with Trafford Alternative Education Provision policies, standards and procedures; to ensure the effective operation of Trafford Alternative Education Provision ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

3.3 All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

4. Breaches

4.1 A breach or suspected breach of policy by a Trafford Alternative Education Provision staff or pupil may result in the temporary or permanent withdrawal of ICT hardware, software or services from the offending individual.

4.2 Inappropriate Contact:

- Report to the organisation manager/e-safety lead/child protection officer who will follow internal policy
- Advise the child or young person on how to terminate the communication and save all evidence
- Contact the child or young person's parent(s)/carer(s)
- Contact the police on (0161) 865 7555
- Log the incident
- Identify support for the child or young person

4.3 Bullying:

- Report to the organisation manager/e-safety lead/child protection officer
- Advise the child or young person not to respond to the message
- Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions
- Secure and preserve any evidence
- Contact the child or young person's parent(s)/carer(s)
- Consider informing the police on (0161) 865 7555 depending on the severity or repetitious nature of the offence
- Log the incident
- Identify support for the child or young person

4.4 Malicious/Threatening Comments Towards a Child, Young Person or Organisation Staff:

- Report to the organisation manager/e-safety lead/child protection officer
- Secure and preserve any evidence
- In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.
- Inform and request that the comments are removed from the site/block the sender
- Inform the police (0161) 865 7555 as appropriate
- Log the incident
- Identify support for the child or young person

4.5 Viewing of Inappropriate/Illegal Websites

- Report to the organisation manager/e-safety lead/child protection officer
- If illegal report to the police on (0161) 865 7555
- If illegal images have been viewed (child pornography/extreme pornography) a member of staff or the police should seize the computer in line with the Association of Chief Police Officer guidelines for computer based evidence (Appendix B) to ensure that evidence can be preserved so that it can be presented in a court of law at a future date if necessary. Even as part of an investigation staff *should not* view images of child pornography or extreme pornography as it is illegal
- Inform the parents
- If inappropriate, refer the child/young person to the AUP that was agreed and reinforce the message
- Contact the filtering software provider/IT section to notify them of the websites viewed
- Decide on an appropriate sanction
- Log the incident in full
- Identify support for the child or young person

4.6 Allegation against a Member of Organisation Staff/Volunteer:

In the case of the above, the Trafford LSCB Child Protection Procedures should be referred to via the TSCB Website.

All allegations should be reported to the manager, police (0161) 865 7555 and Local Authority Designated Officer (LADO) (Phone number (0161) 912 5024) or MARAT-Multi-Agency Referral and Assessment Team (0161 912 5125), as appropriate.

4.7 Whistleblowing:

Employees are often the first to realise that there may be something wrong and it is important that employees raise issues of concern with their own employers so that they can be investigated. Employees who raise concerns are offered some protection through the Public Interest Disclosure Act 1998. Each organisation is advised have their own internal policies on whistleblowing – this should be available via the Intranet or from the Human Resources Department.

4.8 Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For students, reference will be made to the Trafford Alternative Education Provision's Behaviour policy.

5. Incident Reporting

5.1 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Trafford Alternative Education Provision's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals are as follows:

- Lynda Thompson, Executive Headteacher
- Jasmin Boyes, Deputy Headteacher
- Mark Barcroft, Deputy Headteacher

6. Equal Opportunities

6.1 Trafford Alternative Education Provision endeavours to create a consistent message with parents/carers for all students and this in turn should aid establishment and future development of the Trafford Alternative Education Provision's e-safety rules. However, staff are aware that some students may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

7. Staff Usage

7.1 Staff may only create blogs, wikis or other online areas in order to communicate with students using systems approved by the Executive Headteacher.

7.2 Staff are provided with an individual network to staff shared and Trafford email. All staff accessing the schools network are also expected to use a personal password and keep it private.

7.3 Staff are aware of their individual responsibilities to protect the security and confidentiality of the Trafford Alternative Education Provision networks including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Trafford Alternative Education Provision does not use Facebook and Twitter to communicate with parents and carers.

7.4 Staff **are not** permitted to access their personal social media accounts using Trafford Alternative Education Provision equipment at any time.

8. Removable Media

8.1 If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Error! Reference source not found.**'

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

9. E-Safety – Roles and Responsibilities

9.1 As e-safety is an important aspect of strategic leadership within the Trafford Alternative Education Provision, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinators in Trafford Alternative Education Provision are Jasmin Boyes and Mark Barcroft who have been designated this role as a member of the senior leadership team. All members of the Trafford Alternative Education Provision community have been made aware of who holds this post. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Trafford LA CEOP (Child Exploitation and Online Protection) and Childnet.

9.2 Staff and Management Committee Members are updated by the Executive Head, Deputies and all have an understanding of the issues and strategies at Trafford Alternative Education Provision in relation to local and national guidelines and advice.

9.3 This policy, supported by the Trafford Alternative Education Provision's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole Trafford Alternative Education Provision community. It is linked to the following mandatory Trafford Alternative Education Provision policies:

- Child protection
- Health and Safety,
- Behaviour/pupil discipline (including the anti-bullying)
- Personal, Social and Health Education and Citizenship

10. E-Safety in the Curriculum

10.1 ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the students on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

10.2 Trafford Alternative Education Provision Service provides opportunities within a range of curriculum areas to teach about e-safety.

11. Incident Reporting, E-safety Incident Log & Infringements

11.1 Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Trafford Alternative Education Provision's relevant responsible person or e-safety Co-ordinator.

11.2 Keeping an E-safety incident log can be a good way of monitoring what is happening and identify trends or specific concerns (See Appendix 2).

12. Misuse and Infringements

12.1 All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator.

12.2 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Executive Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see Appendix 5)

12.3 Users are made aware of sanctions relating to the misuse or misconduct by Personal, Social and Health Education lessons and assemblies

13. Storage of Images

13.1 Images/ films of children are stored on the Trafford Alternative Education Provision's network.

13.2 Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Executive Headteacher.

13.3 Rights of access to this material are restricted to the teaching staff and students within the confines of Trafford Alternative Education Provision's network or other online resource.

Trafford High School uses CCTV for security and safety. The only people with access to this are the Executive Headteacher, Phil Hatch, Site Manager, Deputy Heads Jasmin Boyes and Mark Barcroft.

14. Personal Mobile Devices (including phones)

14.1 Student's personal mobile devices are not permitted. All are locked away in lockers at THS or TMES

14.2 The sending of inappropriate text messages between any members of the Trafford Alternative Education Provision community is not allowed

14.3 Permission must be sought before any image or sound recordings are made on the devices of any member of the Trafford Alternative Education Provision community

14.4 Where Trafford Alternative Education Provision provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used

14.5 Where Trafford Alternative Education Provision provides a laptop for staff, only this device may be used to conduct Trafford Alternative Education Provision business outside of Trafford Alternative Education Provision

14.6 Staff must never use a hand-held mobile phone whilst driving a vehicle on school business

15. ICT Systems

15.1 All students are expected to use the hardware and software provided with care and respect.

15.2 Students are prohibited from making any changes to the set-up and configuration of the central PCs or to install any software either from CD, Diskette, and USB Flash Drive or via the Internet.

15.3 Only computers (including laptops) owned and supported by the Centre can be used to access the Centre's ICT systems.

16. Use of the Internet

16.1. The centre will, as far as possible, provide adults competent in using the Internet to supervise student Internet sessions and, where appropriate, will monitor and record this usage.

16.2. Internet use within the centre will be driven by clear learning intentions that are set in the context of well framed tasks.

16.3 Access to Newsgroups or 'chat areas' will not be permitted.

16.4 Students should not give out any personal details over the Internet except where specifically approved (e.g. joint projects).

16.5 Students receiving questionable materials must report this immediately to the teacher or member of staff.

17. Unacceptable Usage of ICT, Internet and Email facilities

17.1 The following actions are considered unacceptable.

- Accessing, creating, transmitting, or publishing: any offensive, obnoxious, obscene or indecent messages, images, sounds, data or other material;
- Creating, transmitting or publishing defamatory, violent or abusive material or any material which is likely to cause offence, inconvenience or needless anxiety to others.
- Deliberate unauthorised access to facilities, services, data or resources within the Centre or any other network or service accessible via the Internet.
- Any use of Email or the Internet that would be embarrassing to any individual or the Centre.
- Accessing, creating, transmitting, or publishing any material of a racist nature.

17.2 The Centre's Position

The centre reserves the right to monitor all PC, Email and Internet use and the content of personal network drives and web space. All Emails sent or received by a student and content held within the personal web space may be monitored and reviewed and unacceptable content removed without notice. PC and Internet use will be controlled by a filter limiting the types of site students can visit, and will be monitored with regular checks.

Students should be aware that all Emails and Internet messages sent or received on centre systems are the responsibility of the Centre and the Centre can be held vicariously liable for certain emails/Internet messages that users send.

The Centre will undertake to keep its anti-virus software up to date to ensure that activities are not disrupted by the malevolent actions of others.

Improper use of Emails, Internet and/or personal web space will result in appropriate disciplinary action. Defamatory Emails can result in legal action against the individual.

17.3 The Student's Position

Logging on to the network is seen as an acceptance of the Acceptable Use Agreement (Appendix 1). Any blatant misuse of computers or computer facilities could result in internet access being withdrawn.

18. How to Make a Complaint

If you have a complaints and/ or issues relating to e-safety these should be made to:

- Lynda Thompson Executive Headteacher

Appendix one: Acceptable Use Agreement

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning at Trafford Alternative Education Provision. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like further explanation regarding the Acceptable Use Agreement, please get in touch.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

Yours sincerely



Lynda Thompson
Executive Headteacher

We have discussed this document with.....(child's name) and we agree to follow the e-safety rules and to support the safe use of ICT at Trafford Alternative Education Provision.

Parent/ Carer
Signature:

Pupil Signature:

Year:

Date:

Acceptable Use Agreement: Students

1. I will only use ICT systems in Trafford Alternative Education Provision, including the internet, e-mail, digital video, and mobile technologies for Trafford Alternative Education Provision purposes.
2. I will not download or install software on Trafford Alternative Education Provision technologies.
3. I will only log on to the Trafford Alternative Education Provision network, other systems and resources with my own user name and password.
4. I will follow the Trafford Alternative Education Provision's ICT security system and not reveal my passwords to anyone and change them regularly.
5. I will only use my Trafford Alternative Education Provision e-mail address.
6. I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
7. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
8. I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
9. I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a Trafford Alternative Education Provision project approved by my teacher.
10. I am aware that when I take images of students and/ or staff, that I must only store and use these for Trafford Alternative Education Provision purposes in line with Trafford Alternative Education Provision policy and must never distribute these outside the Trafford Alternative Education Provision network without the permission of all parties involved. This includes Trafford Alternative Education Provision breaks and all occasions when I am in Trafford Alternative Education Provision uniform or when otherwise representing the Trafford Alternative Education Provision.
11. I will ensure that my online activity, both in Trafford Alternative Education Provision and outside of the Provision, will not cause staff, students or others distress or bring the provision into disrepute.

Appendix 2: E-safety Incident Log

Date & Time	Name of Pupil	M/ F	Room and computer number	Details of incident including evidence	Actions and Reason

Appendix 3: Smile and Stay Safe Poster

E-safety guidelines to be displayed throughout the Trafford Alternative Education Provision



Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or Trafford Alternative Education Provision. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

Appendix 4: Information Asset Log

Information Asset	Information Asset Owner	Protective Marking	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Appendix 5: Flowcharts for Managing an e-safety Incident

