



E Safety Policy

Policy Information	
Policy Owner	Matt Bindon
Issue Version	Draft V1
Approving Committee	Interim Academy Board
Adopted Date	January 2024
Review Cycle	Bi Annual
Last Review Date	December 2023
Next Review Date	December 2025

Adoption of the Policy

This Policy has been adopted and reviewed by the IAB of Mount Tamar part of Transforming Futures Trust

Signed

(Chair of Interim Academy Board)

Date 12.01.24

Contents

1 Background/Rationale	3
2 Scope Of The Policy	3
3 Roles and Responsibilities	4
4 Policy Statements	6

1 Background/Rationale

1.1. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately, and safely, is addressed as part of the wider duty of care. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

1.1.1 Access to illegal, harmful or inappropriate images or other content.

1.1.2 Unauthorised access to/loss of/sharing of personal information.

1.1.3 The risk of being subject to grooming by those with whom they make contact on the internet.

1.1.4 The sharing/distribution of personal images without an individual's consent or knowledge.

1.1.5 Inappropriate communication/contact with others, including strangers.

1.1.6 Cyber-bullying.

1.1.7 Access to unsuitable video internet games.

1.1.8 An inability to evaluate the quality, accuracy and relevance of information on the internet.

1.1.9 Plagiarism and copyright infringement.

1.1.10 Illegal downloading of music or video files.

1.1.11 The potential for excessive use which may impact on the social and emotional development and learning of the young person.

1.2 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2 Scope Of The Policy

2.1 This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

2.2 The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

2.3 The school will deal with such incidents within this policy and associated behaviour, safeguarding and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

3 Roles and Responsibilities

3.1 The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

3.1.1 Head teacher and Senior Leaders:

3.1.1.2 The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community.

3.1.1.3 The Head teacher will permit access to specific websites to enable an appropriate curriculum to be accessed using ICT under their professional judgement and express sign off. These sites will also be reported to the local Cluster for monitoring.

3.1.1.4 The Head teacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

3.1.2 Network Manager/Technical staff:

3.1.2.2.1 That the school's ICT infrastructure is secure and is not open to misuse or malicious attack. That the school meets the relevant e-safety technical requirements.

3.1.2.2.2 That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.

3.1.2.2.3 The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

3.1.2.2.4 All requests to allow access to filtered sites will be passed through the Head teacher and then onto to the IT manager for changes to be made.

3.1.2.2.5 Even if a site is deemed suitable by the Head teacher, the IT Manager has the final say with regard to security, safety and impact on systems.

3.1.2.2.6 That he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.

3.1.2.2.7 That the use of the network/remote access email is regularly monitored in order that any misuse/attempted misuse can be reported to the Network Manager and Head Teacher.

3.1.2.2.8 That monitoring software/systems are implemented and updated as agreed in school policies.

3.1.3 Teaching and Support Staff

3.1.3.1 Teaching and support staff are responsible for ensuring that:

3.1.3.1.1 They must ensure their computer is locked if they are away from the device to ensure pupils can't access their documents etc.

3.1.3.1.2 Any request for access to filtered sites are made well ahead of a planned lesson to enable Heads agreement and IT to be informed and changes allowed.

3.1.3.1.3 They have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices.

3.1.3.1.4 They have read, understood and signed the school staff acceptable use policy/agreement (AUP).

3.1.3.1.5 They report any suspected misuse or problem to the Head teacher for investigation/action/sanction.

3.1.3.1.6 Digital communications with pupil/pupils (email/virtual learning environment (VLE)/voice) should be on a professional level and only carried out using official school systems.

3.1.3.1.7 E-safety issues are embedded in all aspects of the curriculum and other school activities.

3.1.3.1.8 Pupils understand and follow the school e-safety and acceptable use policy.

3.1.3.1.9 Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.1.3.1.10 They monitor ICT activity in lessons, extra-curricular and extended school activities.

3.1.3.1.11 They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.

3.1.3.1.12 In lessons where internet use is pre-planned pupils/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

3.1.4 Designated Person for Child Protection/Child Protection Officer

3.1.4.1 The designated person for child protection should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

3.1.4.1.1 Sharing of personal data.

3.1.4.1.2 Access to illegal/inappropriate materials.

3.1.4.1.3 Inappropriate on-line contact with adults/strangers.

3.1.4.1.4 Potential or actual incidents of grooming.

3.1.4.1.5 Cyber-bullying.

3.1.5 Pupils

3.1.5.1 Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use home school agreement, which they will be expected to sign before being given access to school systems (where applicable).

3.1.5.2 Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

3.1.5.3 Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

3.1.5.4 Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices.

They should also know and understand school policies on the taking / use of images and on cyber-bullying.

3.1.5.5 Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

3.1.6 Parents/Carers

3.1.6.1 Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' meetings, newsletters, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

3.1.6.1.1 Endorsing (by signature) the Pupil Acceptable Use home school agreement

3.1.6.1.2 Accessing the school website/social media/on-line pupil/pupil records in accordance with the relevant school Acceptable Use Policy.

3.1.7 Community Users

3.1.7.1 Community Users who access school ICT systems / website / social media / as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

4 Policy Statements

4.1 Education – Pupils

4.1.1 Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach.

4.1.2 The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

4.1.2.1 A planned e-safety programme should be provided as part of ICT/PHS/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.

4.1.2.2 Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

4.1.2.3 Pupils/pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

4.1.2.4 Pupils should be encouraged to adopt safe and responsible use of ICT the internet and mobile devices both within and outside school.

4.1.2.5 Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

4.1.2.6 Staff should act as good role models in their use of ICT, the internet and mobile devices.

4.2 Education – Parents/Carers

4.2.1 Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through:

4.2.1.1 Letters, newsletters, website.

4.2.1.2 Parents meetings.

4.2.1.3 Reference to good practice help guides. 4.3 Education & Training – Staff

4.3.1 It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

4.3.1.1 A planned programme of formal e-safety training will be made available to staff.

4.3.1.2 All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

4.3.1.3 This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings INSET days.

4.4 Technical – infrastructure/equipment, filtering and monitoring

4.4.1 The school/MAT will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

4.4.1.1 School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements.

4.4.1.2 There will be regular reviews and audits of the safety and security of school ICT systems.

4.4.1.3 Servers, wireless systems and cabling must be securely located and physical access restricted.

4.4.1.4 All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually.

4.4.1.5 All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.

4.4.1.6 The “master/administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe).

4.4.1.7 Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

4.4.1.8 The school maintains and supports a managed filtering service. The school has provided enhanced user-level filtering.

4.4.1.9 In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher (or other nominated senior leader).

4.4.1.10 Any filtering issues should be reported immediately to the Network Manager.

4.4.1.11 Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.

4.4.1.12 School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. Remote management tools are used by staff to control workstations and view users’ activity.

4.4.1.13 An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).

4.4.1.14 Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

4.4.1.15 The school infrastructure and individual workstations are protected by up to date virus software.

4.4.1.16 Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

4.5 Curriculum

4.5.1 E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

4.5.1.1 In lessons where internet use is pre-planned, it is best practice that pupils/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.5.1.2 Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

4.5.1.3 It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs or discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

4.5.1.4 Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

4.5.1.5 Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

4.6 Use of Digital and Video Images - Photographic, Video

4.6.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet.

4.6.2 Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

4.6.2.1 When using digital images, staff should inform and educate pupils / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should Page 8 of 16 recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

4.6.2.2 Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

4.6.2.3 Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

4.6.2.4 Pupils must not take, use, share, publish or distribute images of others without their permission.

4.6.2.5 Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

4.6.2.6 Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

4.6.2.7 Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

4.7 Data Protection

4.7.1 Please see the MAT Data Protection Policy for full details.

4.7.2 Staff must ensure that they:

4.7.2.1 At all times take care to ensure the safe keeping of personal data, preventing the risk of its loss or misuse.

4.7.2.2 Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

4.7.2.3 Transfer data using encryption and secure password protected devices.

4.8 Personal Data

4.8.1 As per ACE MAT's Data Protection Policy, personal data can only be stored on the ACE system. Personal data stored must not be transferred to or stored on any portable device or removable media.

4.9 Communications

4.9.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff and other adults				Students/pupils			
	Allowed	Allowed on own device at break	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Personal mobiles may be brought into school		x						x
Use of personal mobiles in lessons				x				x
Use of personal mobiles		X						x
Taking photos on personal phones or other camera devices.				x				x
Use of personal hand-held devices e.g. PDAs		x						x
Use of personal email address in school or on school network				x				x
Use of school email for personal emails				X				X
Use of chat rooms and facilities				x			x	
Use of personal instant messaging		X						x
Use of social networking				X				X
Use of blogs				x				x

4.9.2.1 When using communication technologies the school considers the following as good practice:

4.9.2.1.1 The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

4.9.2.1.2 Users need to be aware that email communications may be monitored.

4.9.2.1.3 Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

4.9.2.1.4 Any digital communication between staff and pupils or parents/carers (email, social media etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

4.9.2.1.5 Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.

4.9.2.1.6 Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

4.9.2.1.7 Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

4.10 Unsuitable/Inappropriate Activities

4.10.1 The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage

User Actions		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images				✓
	Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation.				✓
	Adult material that potentially breaches the Obscene Publications Act in the UK.				✓
	Criminally racist material in UK.				✓
	Pornography.			✓	
	Promotion of any kind of discrimination.			✓	
	Threatening behaviour, including promotion of physical violence or mental harm.			✓	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.			✓	
Using school systems to run a private business			✓		
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards			✓		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.			✓		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords).			✓		
Creating or propagating computer viruses or other harmful files.			✓		
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.			✓		
On-line gaming (educational).	✓				
On-line gaming (non-educational).			✓		
On-line gambling.			✓		
On-line shopping commerce.			✓		
File sharing.		✓			
Use of social networking sites (except for posting on school sites).			✓		
Use of video broadcasting eg YouTube.			✓		

Responding to Incidents of Misuse 4.11.1 It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

4.11.1.1 If any apparent or actual misuse appears to involve illegal activity for example:

4.11.1.1.1 Child sexual abuse images.

4.11.1.1.2 Adult material which potentially breaches the obscene publications act.

4.11.1.1.3 Criminally racist material.

4.11.1.1.4 Other criminal conduct, activity or materials

4.11.2 This must be reported to SLT immediately and all proof kept.

4.11.3 If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

4.11.4 It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Head of Year/other	Refer to Head teacher	Refer to police	Refer to technical support staff for action re filtering/security etc	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction eg detention
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓	✓		
Unauthorised use of non-educational sites during lessons.	✓	✓						✓	
Unauthorised use of mobile phone / digital camera / other handheld device.	✓	✓						✓	
Unauthorised use of social networking / instant messaging / personal email.	✓	✓						✓	
Unauthorised downloading or uploading of files.	✓	✓				✓		✓	
Allowing others to access school network by sharing username and passwords.	✓	✓						✓	
Attempting to access or accessing the school network, using another student's / pupil's account.	✓	✓						✓	

Attempting to access or accessing the school network, using another student's / pupil's account.	✓	✓						✓	
Attempting to access or accessing the school network, using the account of a member of staff.	✓	✓	✓					✓	
Corrupting or destroying the data of other users.	✓	✓	✓	✓				✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.	✓	✓	✓	✓		✓			
Continued infringements of the above, following previous warnings or sanctions.	✓	✓	✓	✓		✓			✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	✓	✓				✓			✓

Pupils	Actions/Sanctions								
Using proxy sites or other means to subvert the school's filtering system.	✓	✓							✓
Accidentally accessing offensive or pornographic material and failing to report the incident.	✓	✓				✓			
Deliberately accessing or trying to access offensive or pornographic material.	✓	✓	✓	✓	✓	✓			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	✓	✓	✓	✓					

Staff	Actions / Sanctions							
Incidents	Refer to line manager	Refer to Head teacher	Refer to local HR	Refer to police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email.	✓					✓		
Unauthorised downloading or uploading of files.	✓	✓				✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓						✓
Careless use of personal data eg holding or transferring data in an insecure manner.	✓	✓						✓
Deliberate actions to breach data protection or network security rules.	✓	✓	✓					✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	✓	✓	✓	✓				✓

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature.	✓	✓	✓	✓				✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils.	✓	✓	✓			✓		
Actions which could compromise the staff member's professional standing.	✓	✓	✓	✓				
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	✓	✓	✓			✓		

Staff	Actions / Sanctions							
	Refer to line manager	Refer to Head teacher	Refer to local HR	Refer to police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Incidents								
Using proxy sites or other means to subvert the school's filtering system.	✓	✓	✓			✓		
Accidentally accessing offensive or pornographic material and failing to report the incident.	✓	✓	✓					
Deliberately accessing or trying to access offensive or pornographic material.	✓	✓	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations.	✓	✓	✓					
Continued infringements of the above, following previous warnings or sanctions.	✓	✓	✓	✓	✓	✓	✓	✓