Thomas Ashton School

E-safety Policy

Approved by Governors:	**Spring 2023**
Date to be reviewed:	**Spring 2024**

Contents:

Statement of intent

1. Legal framework
2. Use of the internet
3. Roles and responsibilities
4. E-safety education
5. E-safety control measures
6. Cyber bullying
7. Reporting misuse
8. Monitoring and review

Appendix A – Staff Acceptable Use Policy

Appendix B – Student Acceptable Use Policy

Statement of intent

At Thomas Ashton School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to mitigate the risk of harm.

1. Legal framework

1.1. **This policy has due regard to, but not limited to:**

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- The Data Protection Act 1988
- DfE (2019) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety 'Education for a Connected World' (2020)
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

1.2. **This policy will be used in conjunction with the following school policies and procedures:**

- Anti-bullying Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement – (it is compulsory for all staff and students to agree and sign the Acceptable Use Agreement)

2. Roles and responsibilities

Governing Body

2.1. The Governing Body is responsible for ensuring that this policy complies with relevant laws and statutory guidance.

2.2. The Governing Board is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

2.3. Members of the Governing Board will hold regular meetings with the e-safety officer and/or relevant Assistant Headteacher to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.

2.4. The Governing Board will evaluate and review this E-safety Policy on an annual basis, considering the latest developments in ICT and the feedback from staff/pupils.

The Headteacher

2.5. The Headteacher, Assistant Headteacher are responsible for ensuring that systems are in place for day-to-day e-safety in the school and managing any issues that may arise.

2.6. The Headteacher is responsible for ensuring that the e-safety officer and any other relevant staff receive CPD to allow them to fulfil their role effectively.

2.7. The Headteacher and Assistant Headteacher will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

2.8. The Headteacher will ensure a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

2.9. The Headteacher and Assistant Headteacher are responsible for ensuring that the school is communicating with parents regularly and updating them on current e-safety issues, advice and control measures.

The wider school and community

2.10. The e-safety officer will regularly monitor the provision and impact of the e-safety curriculum in the school and will provide feedback to the relevant Assistant Headteacher.

2.11. The e-safety officer will identify relevant training for staff as required and will coordinate the teaching of pupils about online safety.

2.12. The Designated Safeguarding Lead will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.

2.13. It is the responsibility of **all staff** to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

2.14. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

2.15. Teachers are responsible for ensuring that e-safety protocols and safe internet access are promoted at all times.

2.16. All staff and pupils will ensure they understand and adhere to the Acceptable Use Agreement, which they must sign and return to the Network Manager/IT Technician.

2.17. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

2.18. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3. Use of the internet

3.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

3.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school has implemented to minimise harmful risks.

3.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. content involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

4. E-safety education

Educating pupils:

4.1. An e-safety programme is delivered across the KS3 curriculum on an annual basis through computing lessons, ensuring that pupils are aware of the safe use of technology both inside and outside of the school. At KS4 all students receive assemblies on e-safety and key elements are covered in computing, workskills and RE.

4.2. Pupils are taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.

4.3. Pupils are taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.

4.4. Pupils are instructed to report any suspicious use of the internet and digital devices to a member of staff.

4.5. Pupils are educated about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

4.6. The school holds e-safety events and assemblies with reference to initiatives such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

Educating staff:

4.7. E-safety training opportunities are available to all staff members, including compulsory whole school training and CPD courses.

4.8. All staff undergo e-safety training to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

4.9. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.10. All staff will be educated on which sites are deemed appropriate and inappropriate.

4.11. Any new staff are required to undergo online e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

4.12. The e-safety officer will act as the first point of contact for staff requiring e-safety advice.

4.13. All staff will be made aware that:

- Any information downloaded must be respectful of copyright property rights and privacy laws.
- Information is stored on the school servers and may therefore be observed by third parties, including student data.
- Downloading explicit or offensive material, unlicensed software or software for personal use, will result in disciplinary response by the school.
- Any information stored on computers must be mindful of confidentiality, data security and not conflict with school or Tameside Council policies.
- Any offensive or inappropriate sites, which escape a block by filtering, must be reported immediately to the e-safety coordinator or ICT Services Team.
- If illegal behaviour by a staff member is suspected, the school has a duty to consult with the police at the earliest opportunity, preserving any potential evidence.

Educating parents:

4.14. E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.

4.15. Parents' evenings, meetings and other similar occasions will be utilised, if necessary, to inform parents of any e-safety related concerns.

5. E-safety control measures

Internet access:

5.1. Internet access is only authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.

5.2. Where a pupil joins Thomas Ashton School who is over the age of 13 and they fully understand what they are consenting to, parents' consent is not required in line with the GDPR; however, the school will notify parents that the pupil has consented independently.

5.3. All users are provided with usernames and passwords and will be instructed to keep these confidential to avoid any other pupils using their login details.

5.4. Management systems are in place to allow members of staff to control workstations and monitor pupils' activity.

5.5. Effective filtering systems are in place to minimise any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.6. Filtering systems can be used which are relevant to pupils, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

5.7. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Headteacher.

5.8. All school systems are protected by up-to-date virus software.

5.9. An agreed procedure is in place for the provision of temporary users, e.g. volunteers.

5.10. Staff are able to use the internet for appropriate personal use during out-of-school hours, as well as break and lunch times.

5.11. Personal use will only be monitored by the safeguarding team (pupils), Network Manager and IT Technician (staff) for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

5.12. If a member of staff is found to be accessing inappropriate content on the internet, they will be prohibited from accessing the BYOD network.

5.13. Thomas Ashton School uses 'Netsupport DNA' to monitor all staff and student online activity with procedures for investigating any misuse (windows, chromebooks/IOS).

Email:

5.14. Pupils and staff are given approved email accounts and are only able to use these accounts.

5.15. The use of personal email accounts to send and receive personal data or information is prohibited.

5.16. No sensitive personal data shall be sent to any other pupils via email.

5.17. No sensitive personal data shall be sent to any other staff or third parties via unencrypted email.

5.18. Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.

5.19. Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.20. Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future. The Network Manager/IT Technician will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

5.21. The use of social media on behalf of the school will be conducted in line with safeguarding guidance.

5.22. Access to social networking sites will be filtered as appropriate.

5.23. There will be no pupil access to social media sites.

5.24. Pupils are regularly educated on the implications of posting personal data online outside of the school.

5.25. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

5.26. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

5.27. Staff are not permitted to publish comments about the school which may affect its reputation.

5.28. Staff are not permitted to access social media sites for personal use during teaching hours using school equipment. Staff should not be accessing social media sites during directed time.

Published content on the school website:

5.29. The Headteacher and Assistant Headteacher will be responsible for the overall content of the website and will ensure the content is checked for appropriateness and accuracy.

5.30. Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

5.31. Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully and will not be posted until authorisation from parents has been received.

5.32. Pupils are not permitted to take or publish photos of others without permission from the individual.

5.33. Staff are able to take pictures for approved use.

5.34. Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:

5.35. The Headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

5.36. Pupils are not permitted to access the school's Wi-Fi system at any time using their own mobile devices and hand-held computers.

5.37. Mobile phones are not permitted to be used during school hours by pupils.

5.38. Staff should not be using personal mobile devices during contact time.

5.39. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use where it is justifiable to do so, and the justification outweighs the need for privacy.

5.40. The sending of inappropriate messages or images from mobile devices is prohibited.

5.41. Mobile devices must not be used by pupils to take images or videos of pupils or staff.

5.42. No mobile device or hand-held computer owned by the school will be used to access public Wi-Fi networks.

5.43. The Network Manager/IT Technician will ensure all school-owned devices are password protected – these passwords will be changed as necessary to ensure their security.

5.44. The Network Manager/IT Technician will review all mobile devices and hand-held computers on a regular basis to ensure all apps are compliant with data protection regulations and up-to-date, and to carry out any required updates.

5.45. The Network Manager/IT Technician will review and request authorisation for any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission from the Network Manager/IT Technician.

5.46. Students should never use the school network to download, load or install any software, shareware or freeware, or load any such software from disks etc, on to school hardware or USB memory sticks.

Network security:

5.47. Network profiles for each pupil and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.

5.48. Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.

5.49. Passwords will expire after a set period to ensure maximum security for pupil and staff accounts.

5.50. Passwords should be stored using non-reversible encryption.

Virus management:

5.51. Technical security features, such as virus software, are kept up-to-date and managed by the Network Manager/IT Technician.

5.52. The Network Manager/IT Technician will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.53. Firewalls will be switched on at all times – the Network Manager/IT Technician will review these on a regular basis to ensure they are running correctly and to carry out any required updates.

5.54. Firewalls and other virus management systems, e.g. anti-virus software, will be maintained and kept fully up-to-date.

5.55. Staff members will report all malware and virus attacks to the Network Manager/IT Technician immediately.

E-safety Team:

5.56. The E-safety Policy will be monitored and evaluated by the school's e-safety team on a regular basis.

5.57. The team will include a member of the SLT, the e-safety officer, the DPO and the Network Manager/IT Technician.

6. Cyber bullying

6.1. For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online.

6.2. The school recognises that both staff and pupils may experience cyber bullying and is committed to responding appropriately to instances that should occur.

6.3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

6.4. Pupils will be educated about online safety through teaching and learning opportunities as part of the KS3 curriculum.

6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

6.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the utmost seriousness.

7. Reporting misuse

7.1. Thomas Ashton School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

7.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

7.3. Concerns regarding a student's online behaviour will be reported to the Network Manager and Designated Safeguarding Lead (DSL).

Misuse by pupils:

7.4. Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.

7.5. Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet will have their internet use suspended.

7.6. Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet.

7.7. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, will be dealt with in accordance with our Child Protection and Safeguarding Policy.

Misuse by staff:

7.8. Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.

7.9. The Headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy and may decide to take disciplinary action against the member of staff.

Use of illegal material:

7.10. In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the Police will be contacted.

7.11. Incidents will be immediately reported to the Internet Watch Foundation and the Police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

7.12. If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and Headteacher will be informed and the Police contacted.

7.13. Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL immediately.

8. Monitoring and review

8.1. This policy will also be reviewed on an annual basis by the Governing Board; any changes made to this policy will be communicated to all members of staff.

8.2. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

Appendix A

Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that 'information systems and ICT' include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff, and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (a strong password has numbers, letters and symbols, with 8 or more characters, password should not be a single word that is found in a dictionary).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the network manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988 and the General Data Protection Regulation (GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or laptop) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school's Data Protection Policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use school equipment to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school's e-safety Policy, (available via the Staff Handbook) which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the designated Child Protection Officer immediately.

- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the GDPR Officer immediately.

- I will not attempt to bypass any filtering and/or security systems put in place by the school.

- If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the school's Service Desk on servicedesk@thomasashton.tameside.sch.uk as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with this AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or Tameside MBC, into disrepute.

- I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practice online, either in school or off site, then I will raise them with the Headteacher.

- I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

The school may exercise its right to monitor the use of information systems, including internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Appendix B

Pupil Acceptable Use Agreement / e-Safety Rules

- I will only use ICT systems in school or on school devices, including the internet, email, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school devices.
- I will not access any material other than that which is directly related to my school work.
- E-mail accounts and approved internet activity should only be accessed when instructed to do so by my teacher or for learning from home.
- I will only log on to the school network/ learning platform with my own user name and password.
- I will follow the school's ICT security systems; I will change my passwords regularly and will not reveal them to anyone.
- I will only use my school email address on school devices.
- I will make sure that all ICT communications with other pupils, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately 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 when in school or my parent/carer when working at home.
- I will not give out any personal information (e.g. name, phone number or address) relating to myself or others.
- I will not arrange to meet anyone I don't know.
- Images of pupils and/or staff will only be taken, stored and used for school purposes in line with school policy and will not be distributed further.
- I will ensure that my online activity, both in school and outside school, will not cause distress to anyone else or bring the school into disrepute.
- I will not deliberately upload or add any images, video, sounds or text that could upset or offend any member of our school community.
- I will respect the privacy and ownership of others' work at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies will be monitored and logged and made available to school staff.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer will be contacted.

The School may exercise its right to monitor the use of information systems, including internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the school's Data Protection Policy. Where it is believed that unauthorised and/or inappropriate use of the school's information system, or unacceptable or inappropriate behaviour may be taking place, the school will invoke its disciplinary procedure. If the school suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.