Online Safety Policy

For the Academies within TAMAT

This Online Safety Policy was approved and adopted by the Trust Board: Spring 2025
It will be reviewed: Sum 2027
Version 25.0

1. RATIONALE

We believe that access to the Internet offers a rich environment for both pupils and staff and that the Internet is an essential element in 21st century life for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. We believe that the potential benefits to pupils from access to information resources far exceed the disadvantages. As part of the children's learning across subjects we will be offering pupils supervised access to the Internet. Before being allowed to use the Internet all pupils must have parental permission to do so.

At TAMAT, we believe that the potential benefits to pupils include the following:

- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use
- Pupils are educated in safe searching when using the Internet, and will be directed to safe and age-appropriate digital resources
- Pupils are taught about how to stay safe on the Internet and how to behave appropriately and responsibly
- Pupils are shown how to publish and present information appropriately to a wider audience
- Pupils are prepared to use online communication tools effectively and safely.

Our Online Safety policy has been written by the school, building on best practice and government guidance.

2. ROLES AND RESPONSIBILITIES

2.1 Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The role of monitoring will be undertaken by the Safeguarding Governing Leads who will:

- Receive regular updates from the Online Safety Lead
- Monitor online safety incident logs

2.2 Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and at least another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made about a pupil. Advice can be found on how to deal with Online Safety concerns on the following websites:
    - https://www.saferinternet.org.uk/blog/advice-schools-responding-online-challenges
    - https://swgfl.org.uk/magazine/5-first-line-responses-to-online-safety-issues/

  All online safety concerns should be reported on CPOMS and passed through to the Online Safety Lead.

- Any online safety concerns about staff should be reported using normal reporting procedures and the Headteacher will respond to these accordingly.
- Staff can use the CEOP report feature for online abuse where concerns are of a nature where police involvement is deemed necessary.
    - https://www.ceop.police.uk/ceop-reporting/
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

2.3 Online Safety Lead

- Our Online Safety Lead is the Headteacher
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority/MAT/relevant body
- Liaises with school technical staff
- Receives reports of online safety incidents (from CPOMS) and creates a log of incidents to inform future online safety developments
- Reports regularly to Senior Leadership Team

3. PROCEDURES / GUIDANCE FOR USE

3.1 Managing access and security

- The school uses a recognised internet service provider or regional broadband consortium
- The school ensures that all internet access has age-appropriate recognised filtering, which is regularly checked to ensure that it is working, effective and reasonable. Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Lead
- The school will ensure that its networks have anti-virus and anti-spam protection that is fully up to date. Antivirus scan reports will be regularly reviewed
- Access to school networks will be controlled by personal passwords except for children, who have limited access to websites using our monitoring and filtering systems.
- School IT systems security is reviewed regularly

3.2 Internet Use

- The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety

- All communication between staff and pupils or families will take place using school equipment and school accounts
- Pupils will be advised not to give out personal details or information which may identify them or their location
- Pupils will be issued with passwords for Purplemash/Kapow Computing and are advised of the implications that may occur if someone finds this out and accesses their account

3.3 Email

- Pupils, staff and Governors may only use approved email accounts on the school IT systems
- Children are taught how to respond appropriately to emails through a whole class demonstration
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.

3.4 Published content, e.g., the school website

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published
- The Headteacher will take overall editorial responsibility and ensure that the content is accurate and appropriate

3.5 Publishing pupils' images and work

- Parents are clearly informed and reminded of the school policy on image taking and publishing onto social media or other online platforms (especially during school performances)
- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press
- Please see school photographic policy for further information

3.6 Videoconferencing

- Videoconferencing whilst at school (usually Microsoft TEAMs or Zoon) will use the educational broadband network to ensure quality of service and security rather than the Internet
- During a school closure period, staff may be using home broadband networks, over which the school has no control regarding filters and security protections. However, the school will provide staff with access to approved platforms for videoconferencing and communication, ensuring that security protocols are maintained. Staff must only use Trust/school-endorsed products when communicating about school matters with one another or with others.

3.7 Home Learning: Risks Online

The school may also use online approaches to deliver training or support. Staff will be aware of the signs and signals of cyberbullying and other online risks and apply the same child-centred safeguarding practices as when children were learning at the school.

- The school continues to ensure appropriate filters and monitors are in place.
- Our Local Academy Board (LAB) will review arrangements to ensure they remain appropriate.
- Children and young people accessing remote learning receive guidance on keeping safe online and know how to raise concerns with the school through the children's page of the website.
- Parents and carers have received information about keeping children safe online with peers, the school, other education offers they may access and the wider internet community. Parents will be offered the following links:
    - Internet matters - for support for parents and carers to keep their children safe online
    - Online safety guidance - for support for parents and carers from the NSPCC
    - Thinkuknow - for advice from the National Crime Agency to stay safe online
    - UK Safer Internet Centre - advice for parents and carers
- Free additional support for staff in responding to online safety issues can be accessed from the Professionals Online Safety Helpline at the UK Safer Internet Centre

3.8 Emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Under normal circumstances, staff will use a school phone where contact with pupils or parents is required. In exceptional circumstances, such as during a pandemic, staff may, with the Headteacher's permission, use their personal mobile phones (number blocked).

3.9 Use of personal equipment

- Mobile phones or devices with imaging and sharing capabilities, including those with cameras will not be used during lessons or formal school time but may be used for communication on outings for necessary contact between the staff and the school office.
- Personal equipment may be used by staff to access the school's IT system provided the use complies with the Online Safety policy and the relevant Acceptable Use Agreement.
- Staff must not store images of pupils or pupils' personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

3.10 Protecting personal data

- The school has a separate Data Protection Policy.

3.11 Authorising Internet access

- As part of their induction, new members of staff are asked to read this policy and to confirm their understanding of and agreement to comply with the 'Acceptable Use of IT Agreement for Staff and Governors' (see Appendix 1)
- All student teachers, work experience trainees, IT technicians and Governors must read and sign the 'Acceptable Use of IT Agreement for Staff and Governors' before using any school IT resource (see Appendix 1).
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- Teaching staff demonstrate effective use of the Internet. Access to the Internet is supervised by adults and children are guided to use appropriate sites
- Parents are asked to sign and return an Internet consent form on entry to the school (see Appendix 3).
- Any person not directly employed by the school will be asked to sign the 'Acceptable Use of IT Agreement for Visitors and Volunteers' (see Appendix 2) before being allowed to access the Internet from the school site.

3.12 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor TAMAT can accept liability for the material accessed, or any consequences of Internet access.

3.13 Handling Online Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- All online safety misuse, illegality or concerns should be reported on CPOMS and passed through to the Online Safety Lead. Advice can be found on how to deal with Online Safety concerns on the following websites:
    - https://www.saferinternet.org.uk/blog/advice-schools-responding-online-challenges
    - https://swgfl.org.uk/magazine/5-first-line-responses-to-online-safety-issues/

3.14 Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety policy and potential IT users will be expected to sign the 'Acceptable Use of IT Agreement for Visitors and Volunteers' (see Appendix 2).

3.15 Introducing Online Safety to pupils

- The school Online Safety programme teaches children about relevant safety issues and instils a set of safe behaviours when accessing the Internet. Online safety lessons are planned and taught regularly throughout the school as part of the Computing curriculum and the Keeping Safe module of the PSHE curriculum.
- Online Safety rules are posted in all school learning areas where computer access for the children is most frequently available (see Appendix 4).
- Pupils are informed that network and Internet use will be monitored.
- Pupils will be taught how to evaluate Internet content.
- The school will seek to ensure that the use of Internet derived material by staff and by pupils complies with copyright law.
- Where possible, pupils are encouraged to verify the information they find online with other sources, e.g. books.
- Pupils are advised never to give out personal details of any kind which may identify them or their location, including uploading photos of themselves in their school uniform.
- Pupils are advised to use nicknames and avatars when using social networking sites and to send kind messages to others as well as to report anything suspicious that they do not like by telling an adult straight away.
- Pupils are taught how to report content that concerns them to a member of teaching staff. The school uses the Windows D function to hide content that children may find concerning, allowing them to seek adult support when needed.
- Pupils are taught to avoid plagiarism and uphold copyright regulations, particularly when using Artificial Intelligence (AI) services.
- The Breck Foundation is invited into school at least once per year to teach children about the dangers online and how to avoid them.

3.16 Vulnerable Pupils

All pupils can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. However, there are some pupils, for example Looked After Children and those with SEND, who may be more susceptible to online harm or have less support from family or friends in staying safe online. As a school we are aware of such vulnerable children and refer to the following documents where necessary to support them:

- Vulnerable Children in a Digital World – Internet Matters https://www.internetmatters.org/about-us/vulnerable-children-in-a-digital-world-report/
- Children's online activities, risks and safety – A literature review by the UKCCIS Evidence Group (section 1.1) https://www.gov.uk/government/publications/childrens-online-activities-risks-and-safety-a-literature-review-by-the-ukccis-evidence-group
- STAR SEND Toolkit

3.17 Staff and the Online Safety policy

- All staff will be given the School Online Safety Policy, and its importance will be explained.

- Staff will receive regular online safety training.
- All staff must sign to confirm that they agree to comply with the 'Acceptable Use of IT Agreement for Staff and Governors' in order to gain access to the school IT systems and the internet on site.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff should report any suspected misuse or problem to the Online Safety Lead for investigation.
- All digital communications with pupils, parents, carers, and others should be on a professional level and only carried out using official school systems. Where staff use Artificial Intelligence (AI), they must only use school-approved AI services (TeachMate AI) for work purposes, ensuring these have been evaluated to comply with organisational security and oversight requirements. In lessons where internet use is pre-planned students/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.
- Staff are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

3.18 Parental support

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues by:

- Ensuring that this policy may also be found on the school website.
- Informing parents about online safety through updates via ParentMail and through the Online Safety Guidance page on the school website.
- Maintaining a list of recommended online safety resources for parents/carers to use in reinforcing messages of online safety outside of school.
- Asking all new parents to sign the parent /pupil agreement when they register their child with the school.
- Encouraging parents to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - digital and video images taken at school events
    - access to parents' sections of the website and online learning platforms such as Purplemash/Kapow Computing
    - Staff must exercise caution when using social media and ensure that any posts related to the school uphold professionalism and confidentiality. Staff should not share or comment on school matters, including pupils, parents, colleagues, or school policies, in a way that could bring the school into disrepute. Any

official communication or representation of the school on social media must be authorised by the leadership team and comply with the school's safeguarding and data protection policies.

- The Breck Foundation conducts an online guidance session with our parents at least once per year.

4. MONITORING EVALUATION AND REVIEW

Our Online Safety Policy has been written by the school, building on best practice and government guidance. The school audits IT use and emergence of new technologies to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

The policy will be reviewed on a 2-year cycle by the Online Safety Lead, the Healthy Schools Lead, teaching staff and Governors on the Local Academy Board.

5. LINKS TO OTHER POLICIES/ USEFUL WEBSITES

- Computing and IT Policy
- Anti Bullying Policy
- Personal, Social and Health Education and Citizenship Policy
- Child Protection and Safeguarding Policy
- www.thinkuknow.co.uk
- https://www.childnet.com/teachers-and-professionals/
- www.net-aware.org.uk
- www.internetmatters.org
- www.parentinfo.org
- www.saferinternet.org.uk

Appendix 1

Acceptable Use of IT Agreement for Staff and Governors

IT and the related technologies such as email, the internet and mobile devices (or any devices with imaging and sharing capabilities) are an expected part of our daily working life in school. This policy is designed to ensure that all staff and Governors are aware of their professional responsibilities when using any form of IT. All staff and Governors are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the Headteacher who is the Online Safety Lead.

- I appreciate that IT includes a wide range of systems, including mobile phones (or any devices with imaging and sharing capabilities), tablets, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.

- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher or Governing Body.

- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.

- I understand that I am responsible for all activity carried out under my username.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that all electronic communications with parents, pupils, staff and Governors, including email, Instant Messaging and Social Networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will ensure that personal data (such as data held on Arbor) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Local Academy Board.

- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network/learning platform without the permission of the Headteacher.

- I will not install any hardware or software without the permission of the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's Online Safety policy and help pupils to be safe and responsible in their use of IT and related technologies. I will promote Online Safety with children in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the Online Safety Lead, the Designated Safeguarding Lead or Headteacher (if different).
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of IT throughout the school.

Full Name…… (Printed)

Job title……

Signature…… Date……

Appendix 2

Acceptable Use of IT Agreement for Visitors and Volunteers

- I understand that I have been given use of the school internet and/or school IT systems in order to carry out a specific job for the school
- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for the purpose for which I have been given access.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will not install any hardware or software without the permission of the Headteacher and Online Safety Lead.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school IT systems
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I understand that if I disregard any of the above then it will be reported to the headteacher serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of IT throughout the school.

Full Name…… (Printed)

Company……

Signature…… Date……

Appendix 3

ACCESS TO THE INTERNET

All pupils use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign agreements to show that the Online Safety Rules have been understood and agreed.

The Golden Rules

- Think then click
- We only use the internet when an adult gives us permission
- We can click on buttons and links when we know what they can do
- We can search the internet with an adult
- We always ask if we get lost on the internet
- We can write polite and friendly messages
- We will not share our Purple Mash passwords
- If you don't like what you see, press Windows D

As part of the school's IT programme, we offer pupils supervised access to the internet. Before being allowed to use the internet, all pupils must have parental permission to do so.

Access to the internet offers a rich environment for both pupils and staff. On-line resources enable our pupils to search for and explore information and engage with a range of exciting resources only available through the internet. At TAMAT we believe that the potential benefits to pupils from access to information resources far exceed the disadvantages.

As a staff, we use electronic information as appropriate for the age of the children. We provide careful guidance and instruction to pupils in the appropriate use of such resources. Only suitable and thoroughly researched electronic resources are used in our school. We recognise that undesirable aspects of the internet do exist and are aware of the potential need for filters, which we have in place, and which allow us to shield our pupils from these aspects.

On-line use in school will be closely supervised by staff. Pupils will be taught to use the internet responsibly. Outside school, families bear the same responsibility for such guidance as they exercise with information sources such as television. Access is a privilege, not a right, and access requires responsibility. But ultimately, parents and guardians are responsible for setting and conveying the standards that their children should follow when using media and information sources. The school supports and respects each family's rights to decide whether or not their children should have access to the internet.

ACCESS TO THE INTERNET – CONSENT & DECLARATION

As the parent or legal guardian of [print child's name]_____, I have read and understood the school's Online Safety rules [see above: **'The Golden Rules'**] and grant permission for my daughter or son to have access to use the internet, school email system, learning platform and other ICT facilities at school.

I know that my daughter or son will be taught about online safety rules as an integral part of the Computing and PSHE curriculum and Online Safety rules are displayed throughout the school in computer use areas. I will take responsibility for guiding my child in the safe and responsible use of the internet and ensure they understand the school online rules.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online safety skills to pupils.

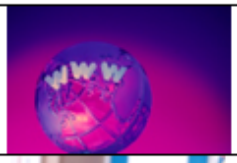
I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their online safety or behaviour online they will contact me.

I understand the school is not liable for any damages arising from my child's use of the internet facilities.

I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online safety.

Parent/Guardian signature _____ **Date** _____

Appendix 4

	Golden Rules Think then click
	We only use the internet when an adult gives us permission
	We can click on buttons and links when we know what they do
	We can search the internet with an adult
	We always ask if we get lost on the internet
	We can write polite and friendly Messages
	We will not share our purple mash passwords
D 	If you don't like what you see, press Windows D