E-Safety Policy at TMS Youth & Arts

Date of last review: 8 March 2024

Date of next review: 8 March 2025

This policy will be reviewed at least annually, and following any concerns and/or updates to national/local guidance or procedures.

1. Mission Statement

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless, TMS Youth & Arts (the Charity) makes full use of these technologies to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. We believe access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use and that the TMS has a duty to provide pupils with quality Internet access. The TMS also recognises that pupils will use these technologies outside TMS and need to learn how to take care of their own safety and security. The Maths Society fully recognises its responsibilities for e-safety, including a responsibility to educate our pupils about the benefits and risks of using new technology and the provision of safeguards and information for all users to enable them to control their online experiences.

This Policy applies to all members of the TMS community (including staff, pupils, volunteers, parents, visitors, community users). All adults, including volunteers, working in or on behalf of the TMS share the responsibility to keep children safe from harm.

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 TMS site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other e-safety incidents covered by this policy, which may take place out of TMS, but is linked to membership of TMS.

The TMS will deal with such incidents within this Policy and associated Behaviour and Anti-Bullying policies and will, where known, inform parents of incidents of inappropriate e-safety behaviour that take place out of school.

2. Aims and objectives

TMS aims to ensure that children are effectively safeguarded from potential risk of harm and that the safety and well-being of children is of the highest priority in all aspects of our work.

Specifically we aim to:

- ensure that all stakeholders are aware of and take seriously their responsibility to promote and safeguard the online safety of children;
-

- use the Internet and other technologies as tools for teaching and learning within the context of educating children and adults in how to use such technology responsibly, giving clear expectations for appropriate use;
- ensure staff and children understand the dangers that can arise and the procedures for dealing with e-safety incidents;
- ensure that TMS Internet access is appropriate for both pupil and adult use and includes filtering appropriate to the age of pupils;
- guide pupils in using technologies and developing skills in ways appropriate to their age and maturity.

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

3. Roles and Responsibilities

3.1 Director and Senior Leaders

The Director (or another member of the Senior Leadership Team) is responsible for:

- ensuring the E-Safety Policy is disseminated and its importance explained;
- ensuring the safety (including e-safety) of members of the TMS Community;
- ensuring relevant staff receive suitable continuing professional development (CPD) to enable them to carry out their e-safety roles and to train other colleagues, as is relevant;
- ensuring that there is a system in place to allow for monitoring and support of those in TMS who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- having familiarity with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Managing all online safety issues and incidents in line with the TMS child protection policy.
- The Director will also address any issues that come to their attention that may relate to use outside school, e.g. of online pornography, cyber-bullying, sexual harassment, peer on peer abuse where these jeopardise the safety and wellbeing of children.

The Director is designated person for child protection and as such should be

- trained in e-safety issues;
- aware of the potential for serious child protection issues to arise from: sharing of personal data; access to illegal/inappropriate materials; inappropriate online contact with adults/strangers; potential or actual incidents of grooming and cyber-bullying.

3.2 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current TMS e-safety policy and practices;
- they report any suspected misuse or problem to the Director
- they respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- digital communications with pupils (email, voice, video) are only on a professional level and carried out using official TMS systems;
- e-safety issues are embedded in all aspects of the Curriculum and other TMS activities;
- pupils understand and follow the TMS E-Safety and Google Classroom agreement;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra-curricular and extended TMS activities;
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices, monitor their use and implement current TMS policies with regard to these devices;
- in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;
- they safeguard the security of their username and password and do not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security and MUST change their password immediately;
- they do not attempt to use any programmes or software that might allow them to bypass the filtering or security systems in place to prevent access to such materials.
- they at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- they 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; they will 'lock' computers when they are not in use using the Windows key + L.

3.3 Pupils

Pupils are expected to:

- use the TMS ICT systems in accordance with the Code of Behaviour and Google Classroom agreement which they will be required to agree to before being given access to TMS systems;
- report abuse, misuse or access to inappropriate materials, once they know how to do so;
- know and understand TMS policies and procedures on the use of mobile phones, digital cameras and hand held devices including the taking or use of images; children are not allowed to use mobile telephones in School.
- understand that cyber-bullying is a form of bullying and will not be tolerated;

- safeguard the security of their username and password and not allow other users to access the systems using their log on details. They should report any suspicion or evidence that there has been a breach of security so their password can be changed;
- understand the importance of adopting good e-safety practice when using digital technologies out of TMS and recognise that the School's E-Safety Policy covers their actions out of TMS, if related to their membership of TMS.

3.4 Parents

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

Parents will be responsible for:
- endorsing the Code of Behaviour and Google Classroom agreement;
- accessing the TMS website in accordance with the relevant TMS Code of Behaviour.

4. E-Safety Education

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates.

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The Diretcor will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

All staff will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

5. Use of Digital and Video Images

- When using digital images, staff are expected to inform and educate 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.
- Members of staff are allowed to take digital or video images to support educational aims, but must follow TMS policies concerning the sharing, distribution and publication of those images. **Such images should only be taken on TMS equipment, the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the TMS into disrepute.
- Photographs published on the Website and Twitter, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on the TMS Website, in association with photographs.
- Permission from parents will be obtained before photographs of pupils are published on the TMS Website

6. Use of Social Networking

TMS blocks access to social networking sites and newsgroups unless a specific use is approved.

7. Filtering Policy

The filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can guarantee 100% protection against access to unsuitable sites. It is therefore important that the TMS has a policy regarding filtering to manage the associated risks and to provide preventative measures which are relevant to the situation at TMS.

8. Password Security

The TMS will be responsible for ensuring that the TMS network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access;
- no user is able to access another's files, without permission (or as allowed for monitoring purposes within TMS's policies);

- access to personal data is securely controlled in line with TMS policy

A safe and secure username/password system is essential if the above is to be established and will apply to all TMS ICT systems, including email.

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to 6nauthorized access or data loss. This should apply to even the youngest of users, even if class logons are being used.

9. Data Protection/ GDPR

The GDPR is based on data protection principles that our TMS must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

Please refer to the Data Protection and GDPR Policy for further detail.

10. Responding to Incidents of Misuse

It is hoped that all members of the TMS 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 use or, very rarely, through deliberate misuse.

If a pupil infringes the E-Safety Policy the incident will initially be referred the Director. After repeated misuse, access to computers and/or the Internet in TMS may be removed for a specific time.

If a staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Director.

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The incident must be immediately reported to the Director, who will seek advice from the Local Authority and report to the police and Social Services as advised. Evidence should be preserved to assist investigation.

11. Handling E-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 Director.
- Complaints of a child protection nature must be dealt with in accordance with TMS child protection procedures (See Safeguarding and Child Protection Policy)
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

12. Monitoring and Review of the Policy

- This Policy will be reviewed annually as part of the TMS's E-Safety Audit and referred to the Board of Trustees should changes be necessary.
- The Director will report annually on e-safety and the implementation of this Policy to the Board of Trustees