Manthan School

E-Safety Policy

AY-2025-26

E-Safety Rationale

In today's digital age, promoting safe and responsible online behaviour is essential to safeguarding students. Our e-safety approach ensures that technology is used positively while protecting learners from risks such as cyberbullying, harmful content, online exploitation, and data misuse.

We believe that:

- **Education is key**: Students are taught how to navigate digital spaces safely, understand privacy, recognize online risks, and act ethically.
- **Safeguarding extends online**: E-safety is part of our duty to protect student wellbeing, both in and out of school.
- **Parents are partners**: We work with families to support safe technology use at home.
- **Monitoring is essential**: Systems are in place to detect and respond to online safety concerns promptly.
- **Children and young people** should never experience abuse of any kind . They should have positive and productive experiences of information and interactive platforms available online
- **Children** should be able to use the internet for education and personal development while staying safe at all times.

Scope of the Policy

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.

Purpose

Safety and Wellbeing of our children and young people is paramount for Manthan. The purpose of this policy is to:

- ensure the safety of children and young people and staff when using the internet, social media or mobile devices.
- provide guidance to staff and volunteers with the overarching principles that outline our approach to online safety
- ensure that, as an organisation, Manthan operates actively and in line with our values and within the law in terms of how children use online devices safely.

We Recognise that:

The online world provides everyone with many opportunities; however, it can also present risks and challenges.

- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Types:

Schools can face a wide range of **online safety (e-safety) issues**, especially as digital tools become more embedded in education. Here's a categorized list of the most common **types of online safety issues** schools may encounter:

1. Cyberbullying

- Harassment, threats, or intimidation through digital platforms.
- Posting harmful or embarrassing content about peers or staff.
- Anonymous bullying via social media, messaging apps, or forums.

2. Inappropriate Content

- Accessing or being exposed to violent, explicit, or otherwise unsuitable content.
- Sharing or downloading offensive material.
- Using school devices to bypass content filters.

3. Online Grooming and Exploitation

- Adults posing as peers to gain children's trust for abusive purposes.
- Coercing children into sharing personal information or inappropriate images.
- Risks associated with online gaming and social networking platforms.

4. Sexting and Image Sharing

- Students sharing explicit images or messages.
- Peer pressure to send inappropriate photos.
- Inappropriate image sharing.

5. Unsupervised Communication Platforms

- Use of chat rooms, messaging apps, or forums without adult supervision.
- Risk of interaction with strangers.
- Engagement in inappropriate conversations.

6. Radicalisation and Extremism

- Exposure or search of extremist content online.
- Influencing vulnerable students through online forums or social media.
- Use of encrypted apps to spread radical ideologies.

Agreed Practices

Mobile Phones

Many new mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Teacher Leaders can bring mobile phones onto the school site where it is seen by the school and parents as a safety/ precaution use. These are handed at the front desk to the Parent Coordinator by 8:45am and collected at the end of the day.
- Staff should not use mobile phones to contact parents/guardians. School Staff will always use the school phone to contact parents/guardians.
- The sending of abusive or inappropriate text message is forbidden.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom or on the playground.
- Staff may use their mobile phones for personal use in the staffroom during the lunch period or before/after school after seeking permission of the TLs.
- Parents cannot use mobile phones on school visits to take pictures of the children.

Laptops/Video Cameras

Pictures, videos and sound are not directly connected to the internet but images are easily transferred.

- Pupils will not use digital cameras, mobile phones or laptops in school unless specifically authorised by SLT member.
- When using digital images, staff should 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.
- 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 can be used but only if other devices are unavailable. These images must be deleted by the end of the day.

- Care should be taken when taking digital/video images that pupils are dressed appropriately and are not participating in activities that put them at risk or bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- 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
- Pupils' full names will not be used anywhere on a website, particularly in association with images.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The school will inform parents/carers and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.

School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, email, telephone and fax numbers.
- Staff and pupils' personal information will not be published.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Parents may upload pictures of their own children on to social networking sites. If the picture includes another child/children, then it is their responsibility to gain permission from that child's parents.
- The governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Active steps and Procedures

The school will organise workshops, activities around being safe online.

The heads, teachers and Safeguarding team will consistently and frequently speak to the learners about safe online platforms and safe online practices.

Online protection apps which will filter and restrict inappropriate websites and guard against online threats will be installed.

For safety of the learners online, **SMOOTHWALL** app will be installed on all devices in the school environment.

The school will liaise with parents through mails, social media post to spread awareness and inclusion of parents in ensuring the safety of the children.

Students will be alerted of the dangerous online platform like Discord, Instagram and Facebook.

Roles and Responsibilities

The IT team will ensure that all devices in the school are secure and protected at all times with Smoothwall.

IT Head will ensure the installation of online protection apps on devices in the school environment

The Senior Leadership Team 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 also support to those colleagues who take on important monitoring roles.

The SLTs will comunicate safe online practices to carers, parents and teachers to extend the scope of onlime safety during orientations, through mails and newsletters.

The Senior Leadership Team, Designated Safeguarding Lead, Deputy Safeguarding Leads will ensure workshops and activities towards educating pupils towards e-safety.

DSL / SLTs/ IT Head/ Teachers will investigate and solve the reported concern

Teaching and non-teaching staff must promptly log e-safety issues on MyConcern portal and report to the TL and DSL

Parents/Guardians support safe internet use at home and communicate any concerns.

Staff Communication and Privacy Guidelines

To ensure the safety, privacy, and professionalism of all interactions within our school community, the following guidelines must be strictly followed by all staff members:

1. **Personal Contact Information**
   Staff members are strictly advised not to share their personal phone numbers or personal email addresses with students and parents
2. **Social Media Boundaries**
   Staff must not accept or initiate friend or follow requests from students (past, present or future) on any social media platforms. Maintaining professional boundaries online is essential.
3. **Sharing of Student Information**
   Changing the names of children whose images are being used in school published material whenever possible (and only using first names if we do need to identify them).Never showing screen shots of video conferencing lessons or meetings that show children's faces and full names. Only designated personnel should handle official communication or posts in press and social media.
4. **Photography at School Events**
   Photographs of students being used by employees for marketing are only taken on school cameras/devices. Images should be saved on a secure server/database and printed copies only used within the school for purposes such as displays, records and learning journals. Images to be used for marketing need to be agreed with parents/carers before use. Visitors and parents/carers should be asked not to use mobiles devices within the school except where permission has been granted to capture images of their own child or children.
   Please see the Child Protection and Safeguarding Policy for fuller guidance.

Reporting

Any online *threat faced or any misuse* by the learner should be promptly reported on MyConcern and reported to the Designated Safeguarding Lead, DDSLs, Teacher Leaders, Vice Principal or the Principal (Depending on the severity of the issue).

All incidents should be logged, investigated, and acted upon promptly by the DSL and Teacher Leaders and the teachers.

Teacher related misuse should be reported to the school Principal

Investigation

Investigation may involve the DSL/ DDSL, TLs, IT Head and teacher (as necessary)

In the situation of online cyberbullying, inappropriate chats , posts, pictures on any online platform support of SLTs, IT Teams, and parents recommended

Review

This policy will be reviewed annually.

~~~~ End of Document~~~~