Headteacher: Mr T Burton, MA (Cantab)

MILLTHORPE SCHOOL
Nunthorpe Avenue
YORK YO23 1WF
T: 01904 686400
F: 01904 686410
E: admin@millthorpeschool.co.uk
W: www.millthorpeschool.co.uk

Millthorpe School

E-Safety Policy

Living the Olympic and Paralympic Values

Table of Contents

Introduction **4**
Responsibilities of the School Community **4**
Responsibilities of the Senior Leadership Team 4
Responsibilities of Teachers and Support Staff 5
Responsibilities of Technical Staff 5
Responsibilities of Students 5
Responsibilities of Parents and Carers 6
Responsibilities of Governing Body 6
Learning and Teaching **7**
Why the Internet and digital communications are important 7
Internet use will enhance and extend learning 7
How parents and carers will be involved **8**
Managing ICT Systems and Access **9**
Filtering Internet access **10**
Learning technologies in school **11**
Using email 12
Using images, video and sound 12
Using blogs, wikis, podcasts, social networking and other ways for students to publish content online 12
Using mobile phones 13
Using new technologies 13
Protecting personal data **14**
The school website and other online content published by the school **15**
Dealing with eSafety incidents **16**
Acknowledgements **18**

Introduction

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience. The e-Safety Policy relates to other policies including those for ICT, bullying, data protection and for child protection.

Responsibilities

Responsibilities of the Senior Leadership Team

- Develop and promote an eSafety culture within the school community.
- Make appropriate resources, training and support available to members of the schoolcommunity to ensure they are able to carry out their roles with regard to eSafety effectively.
- Receive and regularly review eSafety incident logs and be aware of the procedure tobe followed should an eSafety incident occur in school.
- Take ultimate responsibility for the eSafety of the school community.

Responsibilities of the eSafety Coordinator

- Promote an awareness and commitment to eSafety throughout the school.
- Be the first point of contact in school on all eSafety matters.
- Lead the school eSafety group.
- Create and maintain eSafety policies and procedures.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in eSafety issues
- Ensure that eSafety education is embedded across the curriculum.
- Ensure that eSafety is promoted to parents and carers.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on eSafety issues to the eSafety group and SLT as appropriate
- Ensure an eSafety incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff AUP (Acceptable Use Policy).
- Develop and maintain an awareness of current eSafety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed eSafety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Be aware of what to do if an eSafety incident occurs.

- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's eSafety policies and guidance.
- Read, understand and adhere to the school staff AUP.
- maintain a current record of all staff and students who are granted access to school ICT systems
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school ICT system.
- Report any eSafety-related issues that come to your attention to the eSafety coordinator.
- Develop and maintain an awareness of current eSafety issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Students

- Read, understand and adhere to the school student AUP.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by students outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss eSafety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting eSafety.
- Read, understand and promote the school student AUP with your children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
- take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss eSafety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.

- Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's eSafety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by students.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages students to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the eSafety group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety activities.

Learning and Teaching

Why the Internet and digital communications are important

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings.

Internet use will enhance and extend learning

The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.

Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students.

Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- We will provide a series of specific eSafety-related lessons in every year group/specific year groups as part of the ICT curriculum / PSCHE curriculum / other lessons.
- We will celebrate and promote eSafety through whole-school activities.
- We will discuss, remind or raise relevant eSafety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their

actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will remind students about their responsibilities through an end-user AUP which will be displayed when a user logs on.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Include useful links and advice on eSafety regularly in newsletters / on our school website

Managing ICT Systems andAccess

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access.
- Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- Students will access the Internet using an individual log-on, which they will keep secure.
- Students will abide by the school AUP at all times.
- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow students to access the Internet through their log-on. They will abide by the school AUP at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and member of technical support.
- Wireless network access will be secured by a password, this password will only be known to technical support staff.

- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet access

- The school uses a filtered Internet service. The filtering is provided through School Guardian.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafety coordinator/ technical support staff.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafety coordinator/ technical support staff. The school will report this to appropriate agencies including the filtering provider, LA, CEOP or IWF.
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning technologies in school

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The Senior Leadership Team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

	STUDENTS	STAFF
Mobile phones used in lessons	Not Allowed	Not Allowed
Mobile phones used outside of lessons	Not Allowed	Use of camera not allowed
Taking photographs or videos on personal equipment	Not allowed	Not allowed
Taking photographs or videos on school devices	Allowed with teacher permission	Allowed if relates to lesson Must adhere to policy for using student digital images
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Not allowed	Not allowed
Use of personal email addresses in school	Not allowed	Not allowed to communicate with students

Use of school email address for personal correspondence	Allowed with teacher permission	Allowed
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services orsocial networking sites	Not allowed	Not allowed
Use of blogs, wikis, podcasts	Allowed with teacher permission	Allowed

Using email

- Staff and students should use approved e-mail accounts allocated to them by the school,and be aware that their use of the school e-mail system will be monitored and checked.
- Students will be allocated an individual e-mail account for their use in school / classes will be allocated an individual e-mail account for use by students within that class, under supervision of the class teacher.
- Students will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Staff and students are not permitted to access personal e-mail accounts during school.
- Communication between staff and students or members of the wider school community should be professional and related to school matters only using a school approved email account.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately and the appropriate sanction given.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses. An additional staff email address is available via the network manager upon request if staff wish to have an exclusive email address for communication with pupils.

Using images, video and sound

- We will remind students of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will only be created using equipment provided by the school.
- Staff and students will follow the school policy on creating, using and storing digital resources.

- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/students involved.
- If students are involved, relevant parental permission will also be sought before resources are published online.

Using blogs, wikis, podcasts, social networking and other ways for students to publish content online

- Blogging, podcasting and other publishing of online content by students will take place within the schoolwebsite /learning platform.
- Students will not be allowed to post or create content on sites where members of the public have access, including but not limited to, Facebook, mySpace and Bebo.
- Any public blogs run by staff on behalf of the school will be hosted on the learningplatform/school website and postings should be approved by the headteacher before publishing.
- Staff and students will be encouraged to adopt similar safe and responsible behaviours intheir personal use of blogs, wikis, social networking sites and other online publishing outside of school.
- Staff are not permitted to communicate with students via social networking sites.

Using mobile phones

- Mobile phones will not be used during lessons or formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- The use of a camera on a mobile phone, to record video or a digital image is forbidden.
- The use of a mobile phone to record audio is forbidden.
- The use of Bluetooth on a mobile phone is forbidden.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone should be provided and used. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a student or parent

Using new technologies

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafety point of view.

- We will regularly amend the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by students which may cause an eSafety risk.

Protecting personal data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the head teacher, and without ensuring such data is kept secure.

The school website and other online content published by the school

- The school website will not include the personal details, including individual e-mail addresses or full names, of staff or students.
- A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the head teacher before publication.
- The content of the website will be composed in such a way that individual students cannot be clearly identified.
- Staff and students should not post school-related content on any external website without seeking permission first.

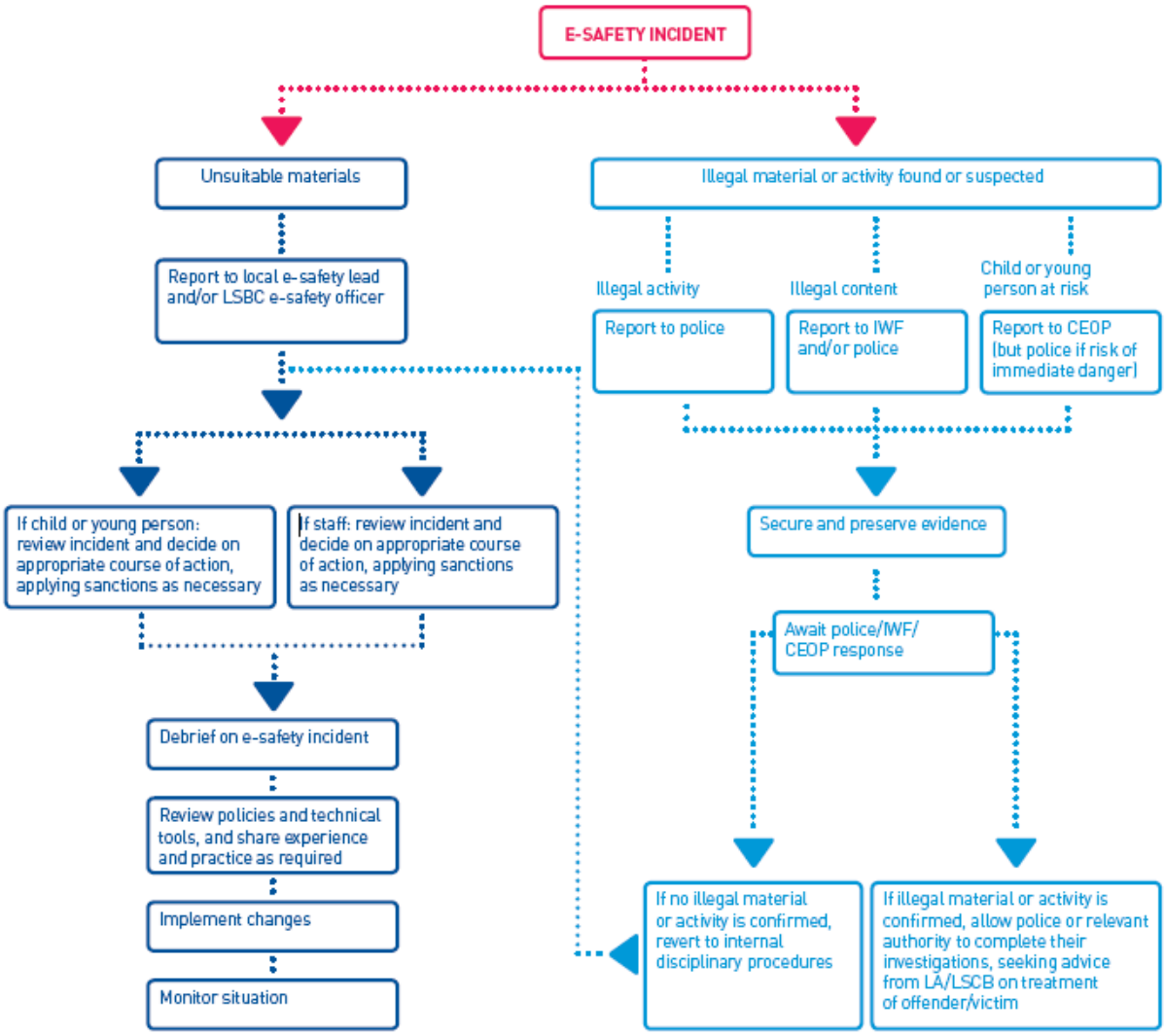
Dealing with eSafety incidents

- The school has procedures in place for dealing with eSafety incidents in school.
- These could range from minor 'classroom disruption', for instance by a student surreptitiously visiting a gaming website during lesson time; to potentially illegal acts ,such as forwarding an obscene image from one mobile phone to another

Incidents that may be encountered include butare not limited to:

- *accessing illegal content deliberately*
- *accessing inappropriate content deliberately*
- *accessing illegal content accidentally and failing to report this*
- *accessing inappropriate content accidentally and failing to report this inappropriate use of personal technologies (e.g. mobile phones) at school*
- *accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed*

- *accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time*
- *downloading or uploading files where not allowed*
- *sharing your username and password with others*
- *accessing school ICT systems with someone else's username and password*
- *opening, altering, deleting or otherwise accessing files or data belonging to someone else*
- *using school or personal equipment to send a message, or create content, that is offensive or bullying in nature*
- *attempting to circumvent school filtering, monitoring or other security systems*
- *sending messages, or creating content, that could bring the school into disrepute*
- *revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission*
- *use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)*
- *transferring personal data insecurely*
- *using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)*


E-SAFETY INCIDENT
Unsuitable materials
Report to local e-safety lead and/or LSBC e-safety officer
If child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief on e-safety incident
Review policies and technical tools, and share experience and practice as required
Implement changes
Monitor situation
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to police
Report to IWF and/or police
Report to CEOP (but police if risk of immediate danger)
Secure and preserve evidence
Await police/IWF/ CEOP response
If no illegal material or activity is confirmed, revert to internal disciplinary procedures
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from LA/LSCB on treatment of offender/victim