Trust Online Safety Policy

This policy reflects the key expectations of all members of the Trust (this includes all Trust staff, and staff at Oakwood High School, Sitwell Junior School and Thomas Rotherham College) with respect to the use of Information Technology (IT) - based technologies. This policy will promote a culture of safe use of digital online media and positive use of IT.

The policy should be read in conjunction with the staff and pupil/student Acceptable Use Agreements General Data Protection Policy and with reference to the 'Child Protection and Safeguarding' policy and procedures.

Introduction

Online safety is about enabling the Trust to benefit as much as possible from the opportunities provided by the Internet and the technologies we use in everyday life. It is not just about the risks, and how we avoid them, it is about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities.

The Trust acknowledges online safety as important and the principles outlined in this policy will be embedded in our approach to learning and using technology. We will work to achieve a balance between using technology to enhance learning and teaching and putting appropriate safeguards in place.

The Trust recognises the benefits of the internet, but believes it is important to balance those benefits with an awareness of the potential risks. We believe this is achieved through a combination of security measures, training and guidance and implementation of associated policies. This policy is designed to show that the Trust is committed to safeguarding and the well-being of its learners.

Responsibilities

Online safety is the responsibility of all in the Trust, everyone has their part to play in ensuring that we can all benefit from the opportunities that technology provides for learning and teaching.

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

All activity across the network and school/college internet will be monitored when using a Trust

device or network, including away from the network such as using a Trust device from home (OHS & SJS Chromebook only).

The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team

1	The Headteacher/Principal is ultimately responsible for online safety provision though day-to-day responsibility may be delegated to appropriate staff.
2	Develop and promote an online safety culture within the school / college.
3	Read, understand, contribute to and help promote the school/college's online safety policies and guidance.
4	Support the development of IT systems to support and monitor online safety.
5	Make appropriate resources, training and support available to members of the Trust to ensure they are able to carry out their roles with regard to online safety effectively.
6	Ensure online safety learning is addressed through the curriculum.
7	Receive and regularly review automated content filtering safety logs and be aware of th procedure to follow up with the user concerned.
8	Take ultimate responsibility for the online safety within the school/college.
9	Ensure that making use of new technologies and online platforms a GDPR Impact assessment is completed and signed off by the head of academy.

Responsibilities of the Safeguarding Lead

1	To promote an awareness and commitment to online safety throughout the school/college.
2	To be the first point of contact in school/college on all online safety matters.
3	To take day-to-day responsibility for online safety within school/college and to have a leading role in establishing policies and procedures. To support the POWER Cadets in their role (Sitwell only). To support the online safety advocates in their role (TRC only).
4	To have regular contact with other online safety committees, e.g. the Local Authority, Local Safeguarding Children Board, the Trust.

5	To communicate regularly with Trust IT Staff to confirm the requirements and system alerts are being received.
6	To develop an understanding of current online safety issues, guidance and appropriate Legalisation.
7	To ensure that all members of staff receive an appropriate level of training in online safety issues.
8	To ensure that online safety education is embedded across the curriculum.
9	To ensure that online safety is promoted to parents and carers.
10	To monitor and report on online safety issues to the senior leadership team.
11	To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
12	To ensure that online incidents are logged on CPOMS.

Responsibilities of the Safeguarding Team

1	Understand the issues surrounding the sharing of personal or sensitive information.
2	Read, understand, contribute to and help promote the school/college's online policies and guidance.
3	Understand the dangers regarding access to inappropriate online contact with adults and strangers.
4	Be aware of potential or actual incidents involving grooming of children.
5	Ensure that all dangers re: potential/actual grooming, cyberbullying, sexting, radicalisation, etc, are responded to appropriately including involvement of external agencies (Police, social care, IYSS, etc). As part of the Prevent Agenda, any suspicious online activity will be referred to the relevant authorities in circumstances where it gives rise to concerns about the safety and well-being of the school/college and/or outside community.

6	Report any issues to the relevant parties.
7	All incidents should be logged in the appropriate Safeguarding system (CPOMS at OHS and SJS)

Responsibilities of Staff

1	Read, understand and help promote the school/college's online safety policies and guidance.
2	Read, understand and adhere to the staff Acceptable Use Policy (AUP).
3	Develop and maintain an awareness of current online safety issues and guidance.
4	Model safe and responsible behaviours in the use of their own technology.
5	Embed online safety messages in learning activities where appropriate
6	Supervise learners carefully when engaged in learning activities involving technology and moderate online content where appropriate.
7	Be aware of what to do if an online safety incident occurs.
8	Embed e-Safeguarding messages in learning activities across all areas of the curriculum.
9	Supervise and guide learners carefully when engaged in learning activities involving technology.
10	Ensure that learners are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
11	Be aware of e-Safeguarding issues related to the use of mobile phones, cameras and handheld devices.
12	Should not communicate with learners and parents using personal mechanisms e.g. a non-work email address, text, mobile phones etc. Staff should not have learners as "friends" on social media.
13	Staff devices such as laptops and Chromebooks may contain sensitive information and allow access to the school/college network so use of them is solely for the member of staff they have been issued.

14	Maintain a professional level of conduct in their personal use of technology at all times.
15	Staff should not post/share any comments that may bring the Trust into disrepute or that may damage its reputation.
16	Ensure that the use of images and photographs do not breach copyright or GDPR regulations and be aware of copyright, GDPR regulations when using online information in general.
17	The use of social networking sites needs to be approved by the CEO.
18	All incidents should be logged in the appropriate Safeguarding system (CPOMS at OHS and SJS, online safety Officer at TRC)
19	Staff should be aware that any reports of them undertaking inappropriate online activity will be investigated and may result in disciplinary action.
20	Online communication should be respectful at all times. Be aware that they are legally liable for anything they post online.
21	Ensure that making use of new technologies and online platforms a GDPR Impact assessment is completed and signed off by the head of academy.

Responsibilities of IT

1	Read, understand, contribute to and help promote the school/college's online safety policies and guidance.
2	Read, understand and adhere to the staff AUP.
3	Ensure that all configuration changes to the technical infrastructure are made upon receipt of authorisation from the CEO and IT Manager and ensure that change management records are maintained.
4	Take responsibility for ensuring that all security, filtering and monitoring systems of the school/college IT system are operational.
5	Report any online safety-related issues that come to your attention (pupil/student issues logged onto CPOMS and staff reported to the Headteacher).
6	Develop and maintain an awareness of current online safety issues, legislation and guidance relevant to your work.
7	Liaise with appropriate support teams on technical issues.
8	All incidents should be logged in the appropriate Safeguarding system (CPOMS at

	OHS and SJS)
9	Secure all administrator level access accounts appropriately with MFA where it is available.
10	Maintain a professional level of conduct in their personal use of technology at all times.
11	Ensure all Web activity, both secure and insecure, is monitored.
12	Ensure that whenever possible all data is encrypted, and access is only granted to authorised users in line with data policy or senior management permissions.
13	Ensure that when making use of new technologies and online platforms, a GDPR Impact assessment is completed and signed off by the head of academy

Responsibilities of learners

1	Read, understand, sign and adhere to the pupil/student AUP
2	Understand school/college policies on the use of mobile phones, digital cameras and mobile devices
3	Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school/college and at home.
4	Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
5	Ensure they attend any relevant safety awareness sessions particularly at the start of the year (TRC only).
6	Take responsibility for their own and each other's safety and responsible use of technology in school/college and at home, including judging the risks posed by the personal technology owned and used by learners outside of school/college.
7	Be wary of divulging personal details online and should look into privacy settings on sites to control access of publicly accessible information.
8	Online communication should be respectful at all times. Be aware that they are legally liable for anything they post online.
9	Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school/college and at home.
10	Be aware of copyright and GDPR regulations when using online information.
11	To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.

12	Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in school/college and at home, or if they know of someone who this is happening to.
13	Discuss online safety issues with family and friends in an open and honest way.
14	Understand where to seek advice or help if they experience problems when using the internet and related technologies, ie, parent or carer, teacher or trusted staff member, Childline, CEOP.
15	Sign an AUP / Home School Agreement which details responsibilities.
16	Understand that if their conduct is unacceptable the matter will be dealt with, within the Behaviour policy of the Trust.

Responsibilities of Parents and Carers

1	Help and support their school/college in promoting online safety.
2	Read, understand and promote the pupil/student AUP with their children.
3	Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school/college and at home.
4	Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
5	Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
6	Model safe and responsible behaviours in their own use of technology.
7	Consult with the school/college if they have any concerns about their children's use of technology.

Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances. See the school consent forms available on the shared network.

Responsibilities of other external groups

1	The school/college will liaise with local organisations to establish a common approach

	to online safety and the safe use of technologies
2	The school/college will be sensitive and show empathy to internet-related issues experienced by learners out of school/college, e.g. social networking sites, and offer appropriate advice where appropriate
3	Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school/college.
4	The school/college will provide an Acceptable Use Policy for any guest who needs to access the school/college computer system or internet on school/college grounds.
5	The school/college will ensure that appropriate levels of supervision exist when external organisations make use of the internet and IT equipment within school/college.

Teaching & Learning

Oakwood High School (OHS)
There is a wide range of learning technologies that are used in school to enhance learning and teaching activities. As a school we will decide which technologies we will allow and which technologies we will restrict or even prevent staff and pupils from using.

Technology Matrix (OHS & TRC)	learners	Staff
Personal mobile phones brought into school/college	Learners allowed but turned off and not used during the day (Not TRC)	S Staff allowed
Mobile phones used in lessons	P learners not allowed	S Staff allowed in emergencies
Mobile phones used outside of lessons	P learners not allowed	S Staff restricted to staff only areas
Taking Photographs or videos on personal equipment	Pupil /students not allowed	S Staff not allowed
Taking Photographs or videos on school/college devices	Pupil /students allowed in accordance with AUP	S Staff allowed in accordance with AUP

Use of personal email addresses in school/college	Pupil not allowed	S Staff not allowed
Use of school/college email address for personal correspondence	Pupil /students not allowed	S Staff not allowed
Use of online chat rooms	Pupil /students not allowed	S Staff not allowed
Use of Instant Messaging Service	Pupil /students not allowed	S Staff not allowed
Use of blogs, Wikis and podcasts	Pupil /students allowed (Educational use only)	S Staff allowed (for professional reasons)
Use of Social networking sites	P Pupil /students have limited access (educational use only)	S Limited Staff allowed (educational use only)

Technology Matrix (SJS)

Communicatlo n Technologies	**Staff and other adults**	**Student/pupil**

	Allowed	Allowed at certain times	Allowed with permission from Safeguarding coordinator/ Head Teacher	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school/college	✓						✓	
Use of mobile phones in lessons			✓					✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices			✓					✓
Use of personal email addresses in school/college,or on school/college network				✓				✓

Use of school/college email for personal emails				✓				✓

Use of chat rooms / facilities		✓						✓
Use of instant messaging		✓					✓	
Use of social networking sites			✓					✓
Use of blogs	✓						✓	

Using email

- Staff and learners should use approved email accounts allocated to them by the school/college and be aware that their use of the school/college e-mail system will be monitored and checked.
- Staff and learners will be allocated an individual email account for their use in school/college.
- Staff and learners will be reminded when using email 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.
- Learners and staff are not permitted to access personal email accounts during school/college.
- Communication between staff and learners or members of the wider school/college community should be professional and related to school/college matters only.
- Any inappropriate use of the school/college email system, or the receipt of any inappropriate messages by a user, should be reported immediately.

Using images, video and sound

- We will remind learners 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/college and at home.
- Digital images, video and sound will only be created using equipment provided by the school/college.
- Staff and learners will follow the school/college AUP 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/learners involved.
- If learners are involved, relevant parental permission will also be sought before resources are published online.
- Staff and learners need to ensure there is no breach of copyright for images/videos downloaded from the internet.
- Staff and learners will not share digital images or videos of learners.

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

We see the potential to use blogs/wikis/podcasts or other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow learners to publish their own content. However, we will ensure that staff and learners take part in these activities in a safe and responsible manner

- Learners will model safe and responsible behaviour in their creation and publishing of online content. For example, learners will be reminded not to reveal personal information which may allow someone to identify and locate them. learners will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.
- Staff and learners will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, and other online publishing outside of school/college.
- Staff and learners should not make posts to social media which will bring the school/college into disrepute.

The school/college website and other online content published by the school/college

- The school/college website will not include the personal details of staff or learners.
- A generic contact e-mail address will be used for all enquiries received through the school/college website.
- All content included on the school/college website will be approved by the assigned senior leader before being made publicly available.
- The content of the website will be composed in such a way that individual learners cannot be clearly identified unless approval by Parents/Carers is given.
- Staff and learners should not post school/college-related content on any external

website without seeking permission first.
Contact details of staff and learners will not be published online.

Action:

All files, communications and internet activity will be subject to monitoring and can be checked at any time. If these statements or other guidance from the school/college are not followed, action may be taken to protect staff and learners, including restricting access to the school/college IT systems. In certain circumstances it may be necessary to confiscate personal equipment.
Any infringement of the above could lead to exclusion, fixed or permanent or in the case of staff, disciplinary action.

Sitwell Junior School (SJS)

1. Managing Digital Content

Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done annually or as part of the enrolment procedure on entry to the school in year 3 or if a new starter in years 4, 5, and 6.

On the school website

- On the school's Twitter account
- On Marvellous Me
- In the school prospectus and other printed promotional material, e.g. newspapers
- In display material that may be used around the school
- In display material that may be used off site
- Recorded or transmitted on a video or via webcam in an educational conference
- Contact details of staff and learners will not be published online.

Parents and carers may withdraw permission, in writing, at any time.

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and deleted from any personal devices. 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 and pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

- Parents may take photographs at school events only with the permission from a member of the senior leadership team. However, they must ensure that only images or videos taken involving their own children are taken.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.
- Sharing of images and videos of learners online is not permitted.

Storage of images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- The school will store images of pupils that have left the school following their departure for use in school activities and promotional resources for no more time than has been agreed with the pupil/parents,
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.
- SLT and administration staff have the responsibility of deleting the images when they are no longer required, or when a pupil has left the school.

2. Teaching & Learning

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupil' lives, not just in school but outside as well, and we believe we have a duty to help prepare our learners to safely benefit from the opportunities the internet brings. We have the responsibility to provide them with the skills and resilience to be able to use the internet safely and understand the consequences of not doing this.

We will begin teaching online safety from Year 3 and this will continue throughout the school. This learning will take place through planned curriculum lessons, as part of the computing curriculum and PSHE. Also, through focused sessions when needed e.g. as part of Safer Internet Day. We will promote and use resources made available online on websites such as ThinkUKnow, and NSPCC.

- We will provide a series of specific safeguarding-related lessons in every year group as part of the computing curriculum, PSHE curriculum, and across topic learning
- We will celebrate and promote Safeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant safeguarding messages with pupils 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.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign and which will be displayed in the IT Suite.

- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored, and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

POWER Cadets will be recruited each year (1 from each class in year 5 and 6). These children will help to keep others safe online, by delivering assemblies every half term. They will receive a lanyard which means they will be identifiable to all children, who will know that they can come to the POWER Cadets with any questions or concerns.

Staff Training

Our staff receive regular information and training on online safety issues in the form of annual updates.

As part of the induction process, all new staff receive the online safety policy and the school's Acceptable Use Policies.

All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Useful Links for Further Information:

Child Exploitation & Online Protection Centre http://www.ceop.police.uk

Internet Watch Foundation http://mobile.iwf.org.uk

DirectGov-'Staying Safe Online' http://www.direct.gov.uk/en/YoungPeople/CrimeAndJustice/KeepingSafe/DG_100276 70

Get Safe Online http://www.getsafeonline.org

UK Safer Internet Centre www.saferinternet.org.uk

SWGFL: Making Sense of the New online safety Standards http://swgfl.org.uk/news/News/onlinonline_safety/Making-Sense-of-the-New-online safety-Standards

Policy Review Frequency	Annual
Policy to be approved by	ELT / Trust Safeguarding Committee
Date of Review	March 2022
Approved by Chair	
Next Review	March 2023
Lead Professional External Review	Ann Abel
Communication	Staff Handbook, Policy Acceptance, Website
Document Location	Staff Handbook, Policy Acceptance, Every Compliance System
PA/HR Officer	Sharon Loftus

Appendix 1 - TRC

Online Safety Reporting Procedure

If this is considered to be Child Protection Safeguarding issue this is referred to the Safeguarding Team who will follow the Safeguarding Policy procedures If this is considered to be a Disciplinary issue, this will follow the Staff Disciplinary procedures, linked to the Safeguarding procedures if applicable.

Any activity considered to be illegal will be referred to the police for investigation