Online Safety Policy (Trust)

This policy reflects the key principles expected of all members of the Trust community 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 online safety policy will be reviewed as per the scheme of delegation or when any significant changes occur with regard to the technologies in use within the trust.

The policy should be read in conjunction with the staff and pupil/student Acceptable Use Policies or ICLT Usage Agreement, GDPR and with reference to the 'Child Protection and Safeguarding' policy and procedures.

Rationale

Online safety is about enabling the Trust Community 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.

An online safety policy allows the Trust to demonstrate that not only do we acknowledge online safety as an important issue for our Trust Community, but also that we have made a considered attempt to embed online safety into our approach to learning, using technology.

An online safety policy demonstrates how we work to achieve a balance between using technology to enhance learning and teaching and putting appropriate safeguards in place.

Introduction

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 pupil/students.

Responsibilities of the School/College Community

We believe that online safety is the responsibility of the whole school/college community and that everyone has their part to play in ensuring all members of the community are able to 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 pupil/students but everyone within our Trust Community, lies in effective education. We know that the internet and other technologies are embedded in our pupil/students' lives, not just in school/college but outside as well, and we believe we have a duty to help prepare our pupil/students to safely benefit from the opportunities the internet brings.

All electronic communication and activity across the network and internet will be monitored when using a Trust device or network, including away from the network such as using a Trust device from home.

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 the online safety coordinator.
2. Develop and promote an online safety culture within the Trust Community.
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 Community 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 online safety incident logs and be aware of the procedure to be followed should an online safety incident occur in school/college.
8. Take ultimate responsibility for the online safety within the Trust Community.

Responsibilities of the Online Safety Officer (if applicable)
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.
4. To support the POWER Cadets in their role (Sitwell only). To support the online safety advocates in their role (TRC only).
5. To have regular contact with other online safety committees, e.g. the Local Authority, Local Safeguarding Children Board, Trust.
6. To communicate regularly with Trust IT Staff
7. To communicate regularly with the designated online safety governor
8. To create and maintain online safety policies and procedures
9. To develop an understanding of current online safety issues, guidance and appropriate legislation.
10. To ensure that all members of staff receive an appropriate level of training in online safety issues
11. To ensure that online safety education is embedded across the curriculum
12. To ensure that online safety is promoted to parents and carer
13. To monitor and report on online safety issues to the senior leadership team
14. To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
15. To ensure that an 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. Be aware of and understand cyberbullying, radicalisation – and the use of social media for these purposes.
6. Ensure that all dangers re: potential/actual grooming, cyberbullying, sexting, radicalization, 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.
7. Report any issues to the relevant parties.
8. All incident 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)/ICLT Usage Agreement.
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 pupil/students 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 pupil/students carefully when engaged in learning activities involving technology.
10. Ensure that pupil/students 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 pupil/students and parents using personal mechanisms eg a non-work email address, text, mobile phones etc. Staff should not have pupil/students as "friends" on social media.
13. Staff devices such as laptops and Macbooks 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. School/college issued devices, such as iPads, remain the responsibility of the staff member they have been issued. If they are shared at home they remain the responsibility of the staff member.
15. Maintain a professional level of conduct in their personal use of technology at all times.
16. Staff should not post/share any comments that may bring the Trust into disrepute or that may damage its reputation.
17. 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.
18. The use of social networking sites and other sites not hosted by the college may be used only where a risk assessment is completed with the Online Safety Officer and signed by the Principal. (TRC only). Staff should ensure that settings are set to private.
19. All incident should be logged in the appropriate Safeguarding system (CPOMS at OHS and SJS, online safety Officer at TRC)
20. Staff should be aware that any reports of them undertaking inappropriate online activity will be investigate and may result in disciplinary action.

21. Online communication should be respectful at all times. Be aware that they are legally liable for anything they post online.

Responsibilities of IT Technical Department
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. Support the school/college in providing a safe technical infrastructure to support learning and teaching.
4. Take responsibility for the security, filtering and monitoring of the school/college IT system.
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 people and organisations on technical issues.
8. All incident should be logged in the appropriate Safeguarding system (CPOMS at OHS and SJS)
9. Secure all administrator level access accounts appropriately.
10. Ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school/college.
11. Ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
12. Ensure that controls and procedures exist so that access to school/college-owned software assets is restricted.
13. Maintain a professional level of conduct in their personal use of technology at all times.
14. Ensure all Web activity, both secure and insecure is monitored.
15. 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.
16. Ensure that making using of new technologies and online platforms a risk assessment is completed and signed off by the Principal (TRC only).

Responsibilities of Pupil/Students
1. Read, understand, sign and adhere to the pupil/student AUP/ICLT Usage Agreement.
2. Understand school/college policies on the use of mobile phones digital cameras and mobile devices
3. Understand school/college policies regarding cyberbullying
4. Take responsibility for learning about the benefits and risks of using the internet and other technologies; in school/college and at home.
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 others' 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 pupil/students 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, 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 you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school/college and at home, or if you 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 a Home school/college 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 your school/college in promoting online safety.
2. Read, understand and promote the pupil/student AUP with your 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 your own use of technology.
7. Consult with the school/college if you have any concerns about your children's use of technology.

Sitwell only:
To agree to and sign the home-school/college agreement which clearly sets out the use of photographic and video images outside of school/college
To sign a home-school/college agreement (The Sitwell Promise) containing the following statements:

We will support the school/college approach to online safety and not deliberately upload or add any images, videos, sounds or texts that could upset or offend any member of the school/college community.

We will support the school/college's stance on the use of IT and IT equipment Images taken of pupil/students at school/college events will be for personal use only and not uploaded or shared via the internet

Parents may not take photographs at school/college events, unless they have been given permission from staff. If they have been given permission from staff, photos must be of their child only.
Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to the school/college
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 school/college enrolment form/permissions document on staff shared network

Responsibilities of Governors

1. Read, understand, contribute to and help promote the school/college's online safety policies and guidance.
2. Have an understanding of the benefits and risks of the Internet and common technologies used by pupil/students.
3. Develop an overview of how the school/college IT infrastructure provides safe access to the Internet.
4. Be aware of how the school/college encourages pupil/students to adopt safe and responsible behaviours in their use of technology in and out of school/college.
5. To support the work of the Safeguarding group in promoting and ensuring safe and responsible use of technology in and out of school/college including encouraging parents to become engaged in online safety activities

.**Responsibilities of other external groups**

The school/college will liaise with local organisations to establish a common approach to online safety and the safe use of technologies

The school/college will be sensitive and show empathy to internet-related issues experienced by pupil/students out of school/college, e.g. social networking sites, and offer appropriate advice where appropriate

Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school/college

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

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)	Pupil/Students	Staff
Personal mobile phones brought into school/college	Pupil/students allowed but turned off and not used out during the day (Not TRC)	Staff allowed
Mobile phones used in lessons	Pupil/students not allowed	Staff allowed in emergencies
Mobile phones used outside of lessons	Pupil/students not allowed	Staff restricted to staff only areas
Taking photographs or videos on personal equipment	Pupil /students not allowed	Staff not allowed
Taking photographs or videos on school/college devices	Pupil /students allowed in accordance with AUP	Staff allowed in accordance with AUP
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Pupil /students not allowed	Staff restricted to staff only areas
Use of personal email addresses in school/college	Pupil not allowed	Staff allowed
Use of school/college email address for personal correspondence	Pupil /students allowed at certain times	Staff allowed
Use of online chat rooms	Pupil /students not allowed	Staff not allowed
Use of instant messaging services	Pupil /students not allowed	Staff not allowed
Use of blogs, Wikis and podcasts	Pupil /students allowed (Educational use only)	Staff allowed (for professional reasons)
Use of Social networking sites	Pupil /students have limited access (educational use only)	Staff allowed (educational use only)

Technology Matrix (SJS)

Communication 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
1. Staff and pupil/students should use approved e-mail 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.
2. Staff and pupil/students will be allocated an individual e-mail account for their use in school/college.
3. Staff and pupil/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.
4. pupil/students are not permitted to access personal e-mail accounts during school/college.
5. Communication between staff and pupil/students or members of the wider school/college community should be professional and related to school/college matters only.
6. Any inappropriate use of the school/college e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of SLT immediately.

Using images, video and sound
1. We will remind pupil/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/college and at home.
2. Digital images, video and sound will only be created using equipment provided by the school/college.
3. Staff and pupil/students will follow the school/college AUP on creating, using and storing digital resources.
4. 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/pupil/students involved.
5. If pupil/students are involved, relevant parental permission will also be sought before resources are published online.
6. Staff and pupil/students need to be ensure there is no breach of copyright for images/videos downloaded from the internet.

Using blogs, wikis, podcasts, social networking and other ways for pupil/students 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 pupil/students to publish their own content. However, we will ensure that staff and pupil/students take part in these activities in a safe and responsible manner

1. Pupil/students will model safe and responsible behaviour in their creation and publishing of online content. For example, pupil/students will be reminded not to reveal personal information which may allow someone to identify and locate them. pupil/students will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.
2. Staff and pupil/students 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.
3. Staff and pupil/students should not make posts to social media which will bring the school/college into disrepute.

Using mobile phones
1. Personal mobile phones are not permitted for use during school/college time.
2. Occasionally staff members may be required to use a mobile phone for school/college duties, for instance, in case of emergency during off-site activities and then for contacting pupil/students or parents.

Any misuse of mobile phones for the purpose of bullying sharing inappropriate images will be dealt with in accordance with the school/college Behaviour Policy.

The school/college website and other online content published by the school/college
1. The school/college website will not include the personal details of staff or pupil/students.
2. A generic contact e-mail address will be used for all enquiries received through the school/college website.
3. All content included on the school/college website will be approved by assigned senior leader before being made publically available.
4. The content of the website will be composed in such a way that individual pupil/students cannot be clearly identified unless approval by Parents/Carers given.
5. Staff and pupil/students should not post school/college-related content on any external website without seeking permission first.

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 pupil/students, 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
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

·   Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

·   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.

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 for no more than 3 years following their departure for use in school activities and promotional resources.

·	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 has 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 pupil/students 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. through P4C or as part of Safer Internet Day. We will promote and use resources made available online on websites such as ThinkUKnow, and NSPCC. In addition to sessions planned for children, we will hold workshop sessions for parents, with the support of Rawmarsh CLC, once per term.

·	We will provide a series of specific safeguarding-related lessons in every year group as part of the computing curriculum, PSHE curriculum, P4C 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 and termly staff meetings.

·   Training is also accessed offsite at Rawmarsh CLC by the online safety Coordinator and other key members of staff, such as SLT and Learning Mentors.

·   As part of the induction process, all new staff receive information and guidance on 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

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.