Online Safety Policy 2022/2023

Approved by: **Dave Higgens** **Chair of Governors**	**Date:** March 2023
Last reviewed on: **March 2023**	
Next review due by:	March 2024

1. Introduction

Traditionally the term online Safety was synonymous with protection against Sexual Exploitation and Cyberbullying however in 2021 professionals should be aware that this term additionally covers education, advice and protection around areas including, Criminal Exploitation, Radicalisation, Cybersecurity and Health and Wellbeing all of which have a large 'online' component.

The continual growth and widespread use of the Internet, mobile phone and gaming technology has significantly enhanced our ability to communicate, share information, images, be entertained, and learn. There are enormous benefits to using digital media, which has revolutionised our lives. It is important to recognise that digital technology is integral to the lives of children and young people in today's society and that the majority have widespread access to the internet on their mobile phones, tablets and gaming devices via WiFi. Much of their WiFi access is free and unrestricted both publicly and in the home. This can make parental control of content and contact very challenging.

Many of these technologies are used as powerful tools for teaching and learning in schools and other educational settings. Within school children are heavily protected in the online environment, and much work has already been done in our school with staff, pupils and parents/carers to raise awareness of the risks associated with using digital technology. The boundaries of technology reach far beyond the school gate and we have a responsibility, therefore, as part of the wider duty of care, to safeguard and promote the welfare of children and young people and help them develop the skills to look after themselves both in and out of school. We also have a responsibility to take action against those who harm children and young people via digital technology.

Online safety awareness has been extended to some Children's Services and partner agencies who work with children and young people. The challenge is to roll this out to the wider community whilst keeping abreast of new technological developments and to empower parents and other responsible adults so that they can concentrate on the behaviours of children and young people online which expose them to increased risk rather than the technology itself. As professionals it is important that we refrain from vilifying individual apps or games, which change frequently but rather concentrate on the behaviour within the app or game that increases risk. The Covid 19 pandemic has undoubtedly changed the online landscape for us all but particularly our young people. Going forward it will be increasingly necessary to adopt contextual safeguarding techniques within the online space and have much more nuanced conversations with young people about their behaviour and being safe. As in the real world we must not blame young people for their exploitation online particularly if they are in an age inappropriate space. The fault always lies with those who choose to exploit or abuse children.

This procedure is about safeguarding children and young people in a digital generation. However, due to the vulnerability of some adult practitioners to being cyberbullied and

the exponential use of social media, guidance is also provided for practitioners to be able to safeguard themselves online.

2. Purpose

The effects of abuse suffered by children and young people via digital technology are the same as that which occurs via personal contact. Indeed, some physical and sexual abuse may occur as a result of initial contact online via digital technology or indeed can be wholly carried out online. However, the impact may be more severe in some cases as the abuse can take place in the home, where a child or young person should feel safe. Therefore, it is **the responsibility of all practitioners to ensure they know what to do if they suspect a child or young person is involved, or at risk of involvement, either as a victim or perpetrator, of exploitation of any type online or via digital technology**. The purpose of this procedure is, therefore, to provide guidance to all those working with children, young people and their families in Sheffield.

3. Aims

The aims of this procedure are as follows:

- To define the different types of digital technology and the risks they present to children and young people;
- To provide guidance to practitioners regarding the safeguards that should be in place to protect children and young people using digital technology, within our school
- To provide information about some risk indicators in relation to the internet and digital technology;
- To provide guidance to practitioners as to what action they should take if they are concerned about a child or young person related to digital and interactive technology, and provide information about legislation;
- To provide guidance to practitioners about how to minimise risk for themselves, so that they do not inadvertently leave themselves open to allegations of practitioner misconduct from children and young people, or their parents / carers.

4. Definition

4.1 Online Safety

This is the generic term that refers to raising awareness about how children, young people and adults can protect themselves whilst using digital technology and online environments, and also interventions that can reduce the level of risk for children and young people.

Please see **NSPCC Learning on Online Abuse** for more information.

Online Safety covers the following areas – Please see **UK Council for Child Internet Safety - Education for a Connected World** for more information.

- Health and Wellbeing, Sleep, Body image, Balance of on and offline activity, Mental Health, Purchasing drugs online, Accessing positive health information and identifying misinformation.
- Cyberbullying Please see **NSPCC Bullying and Cyberbullying Learning**;

For those practitioners who may have less experience of using digital technology the **UK Safer Internet Centre Parents Guide to Technology** page provides a wealth of technical background information and NSPCC **Net Aware** gives advice about the operation and safety features in individual Apps. Also the parents' sites listed in the guidance section will also be of use for general information.

5. Legislation

It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the event of an online issue or situation.

Online Safety Policy

1. Introduction

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology - including computers, mobile phones and online games - and provides safeguards and awareness for users to enable them to control their online experiences.

This Online Safety Policy provides guidance to our staff to safeguard our children. It also operates in conjunction with other policies including Behaviour, Bullying, Curriculum, Data Protection and Security. Model Online Safety Policies for Schools and for Early Years Education Providers are available on the Sheffield Children Safeguarding Partnership website.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, children and young people; encouraged by education and awareness raising and made explicit through published policies;
- Support and guidance for parents, giving them the knowledge and confidence to be able to supervise their child's use of digital and interactive technology;
- Sound implementation of Online Safety policy in both administration and raising awareness, including secure network design and use;
- Safe and secure broadband filtering and monitoring solutions e.g. Smoothwall where applicable, or other firewalls;
- Network standards and specifications.

This policy provides guidance for agencies in relation to these issues. It specifically relates to the use of computers in organisations; it does not cover the use of mobile phones by children. Please see the Acceptable use of ICT and Digital Technology Policy.

The responsibility for Online Safety lies with the Designated Safeguarding Leads – Tracey Naylor and Hayley Wright.

2. Benefits of the Internet for Children and Young People

The purpose of Internet use in organisations is to promote the wellbeing and achievement of children, to support the professional work of staff and to enhance our school's management information and administration systems.

Internet use is an essential element in 21st century life for education, business and social interaction. It is also part of the statutory curriculum from the age of 5 years. Therefore our school has a duty to provide children with quality Internet access and equip them with the skills to be safe whilst using digital and interactive technology.

Benefits of using the Internet include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between children and young people world-wide;
- Access to experts in many fields for children and young people and staff;
- Professional development for staff through access to national developments, educational materials and effective professional practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of;
- Networks and automatic system updates;
- Exchange of professional issues and administration data between local, regional and national organisations;
- Access to learning and communication wherever and whenever convenient.

At Rivelin, Internet access is designed expressly for children and young people's use and includes filtering appropriate to the age of children and young people.

Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning and personal development activities.

Staff will guide children in on-line activities that will support learning outcomes, which are planned according to their age and maturity.

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

3. Managing Internet Use in School

This section provides guidance about how to manage the use of the Internet in the school. Children should be provided with guidance in computer rooms.

Authorised Internet Access

The school will maintain a current record of all staff and children and young people who are granted Internet access.

All staff must read and sign the 'Acceptable Use Policy' or similar before using the organisation's ICT resource.

Parents / carers will be informed that children and young people will be provided with supervised Internet access.

Parents / carers will be asked to sign and return a consent form for children and young people's access.

World Wide Web

If staff or children and young people discover unsuitable sites, the URL (address), time, content must be reported to the designated manager or helpdesk within the school via the Online Safety coordinator or network manager.

The school will ensure that the use of Internet derived materials by children and staff complies with copyright law.

Children and young people should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

E-mail

Children may only use approved e-mail accounts on the organisation system.

Children must immediately tell a member of staff if they receive offensive e-mail.

Children must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Access to external personal e-mail accounts may be blocked.

E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on organisation headed paper.

Children, young people and their families should only contact members of staff of organisations using business email addresses or telephone numbers. This includes staff who they knew before becoming service users of the organisation. Any exceptions to this should be discussed with managers within the organisation. This is to safeguard the children, young people, their families and the member of staff from allegations of misconduct.

Social Networking

School will manage/block/filter access to social networking sites as appropriate for children and staff.

Children and staff are advised never to give out personal details of any kind which may identify them or their location.

Children and staff are advised to consider whether the photos they upload to any social network are appropriate to be seen in a public space and to control who can access their images.

Children are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block and report unwanted communications. They should be encouraged to invite known friends only and deny access to others.

Children and their families should not contact members of staff via social networking sites. Staff should not accept them as friends on social networking sites and should be encouraged to review information posted about them on such sites.

Filtering

The school will work with identified colleagues within SCC to ensure suitable filtering and monitoring systems are installed and used as effectively as possible.

Virus protection will be installed and updated regularly.

Security strategies should be discussed with the organisation's senior management team.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

4. Publishing Images and Work on the Internet

Photographs that include children will be selected carefully.

Children and young people's full names will not be used anywhere on the school's Web site or Blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of their children are published on the School's Web site – See Rivelin Primary 'Use of Cameras and Images Policy.'

Work can only be published with the permission of the children and their parents or carers.

5. Managing other Technologies

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

Children should not use mobile phones during time spent with staff from the school, without prior agreement from a relevant member of staff, e.g. teacher or key worker.

If children send abusive or inappropriate text messages, this will be dealt with by a relevant member of staff, e.g. a teacher or key worker and may result in action being taken.

Staff will be issued with an organisation phone where contact with children is required. They should not use their personal mobile phone to contact children or their families.

6. Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international access available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a school's computer. Neither the organisation nor Sheffield Safeguarding Children Partnership can accept liability for the material accessed, or any consequences of Internet access.

Any child or member of staff who inadvertently accesses inappropriate sites or materials should immediately report the incident to the designated Online Safety lead officers- Tracey Naylor and Hayley Wright and ICT Manager in the organisation.

The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

7. Handling Online Safety Complaints

Complaints of Internet misuse will be dealt with by the line manager as per the school's code of conduct.

Any complaint about staff misuse must be referred to a member of the Senior Leading Team. This may either be the complainant's line manager, or the manager of the member of staff about who the complaint is being made. This may invoke the **Sheffield Children Safeguarding Partnership, Allegations against Staff, Volunteers or Carers Protocol**.

Children and parents / carers will be informed of the complaints procedure.

Discussions will be held with South Yorkshire Police to establish procedures for handling potentially illegal issues. They can be contacted on 0114 220 2020.

8. Communicating the Contents of this Policy

Children

Rules for Internet access will be posted in all networked rooms.

Children and young people and staff will be informed that Internet use will be monitored.

Staff

All staff will be given a copy of this policy, its importance explained and asked to sign the acceptable use policy for staff.

Staff should be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents / Carers

Parents / carers' attention will be drawn to this Online Safety Policy in newsletters and the school's website.

Appendix 2: Indicators of Risk of Sexual Exploitation via Digital and Interactive Technology

At Risk

- Spending increasing amount of time on social networking sites and messaging apps;
- Unexplained increased mobile phone credits or new mobile phone;
- New contacts with people out of city;
- Spending increasing amounts of time with on line friends and less time with friends from school or neighbourhood;
- Going on line during the night;
- Being secretive. Using mobile phone for accessing social networks;
- Unwilling to share /show on line contacts;
- Concern that a young person's online friendship has developed into an off line relationship;
- Concern that inappropriate images of a young person are being circulated via the internet.
- Arranging to meet people they have met on line;
- Concern that a young person is having an online relationship;
- Concern that a young person is being coerced to provide images or to perform sexual acts via webcam;
- Sharing of inappropriate images amongst friends.
- Concerned that a young person is being bribed by someone for their inappropriate on line activity;
- Concern that a young person is selling images via the internet for money;
- Concern that a young person is being drawn into providing increasingly provocative/sexualised images in exchange for payment or from fear of activity being revealed to significant adults;
- Negotiating a price for sexual activity/images;
- Concern that a young person is selling sexual services via the internet.

Appendix 3: Guidance for Practitioners to Minimise the Risk of Misconduct Allegations related to Acceptable Use of Digital and Interactive Technology Policy

At Rivelin, we have a Code of Conduct Policy, which this guidance does not intend to replace. It is guidance that relates specifically to helping professionals put safeguards in place to minimise the risk of any allegations of professional misconduct related to the use of digital technology and social media (e.g. Social networks such Facebook, Twitter, Linkedin, online gaming, etc.)

This guidance relates to all children up to the age of 18, whether or not they, or their families, are current or former pupils, students/service users. It is appreciated that you may have personal friends or the children of friends who are under the age of 18. But at all times you should ensure that you treat all those under the age of 18 with the respect they deserve, whoever the child or young person is.

You should always be mindful not to put yourself in a situation that may comprise you or be misinterpreted either by the child or young person, their friend, parent or carer, or any other person. This includes both personal and professional situations. It should be remembered that careless and inappropriate action in a personal setting, whether intended or not, could have significant implications for your professional life.

There are few professionals who have allegations of professional misconduct related to digital technology or social media made against them. However, the impact of either an allegation or cyberbullying can be significant, both personally and professionally. Taking a few steps to be pro-active in minimising any risk to yourself, whilst you may think it unnecessary, is worth taking to avoid future complications.

Remember: as a professional working with children and young people, or their families, you may be vulnerable to have an allegation made against you or being the victim of cyberbullying. Sometimes this is a result of communication or a situation being misconstrued. Other times this may be an act of revenge taken against you for an incident that has resulted through your professional practice. It may also be that someone, through having complex needs of their own, may develop an unhealthy interest in you as a person.

Therefore the following steps are recommended to all professionals, and trainees who are or will be working with children, young people or their families.

Ten Steps to Minimise Professional Risk

1. You should fully appreciate that the onus is upon you and not the child or young person to distance yourself from any potentially inappropriate situation;
2. Regularly review all content about yourself on social networking sites, such as Facebook, Twitter etc. Particularly consider removing any personal information or photographs which could be manipulated and used against you;
3. Regularly review your privacy settings on all social networking accounts;
4. Do not give personal information such as email addresses or mobile telephone numbers to anyone who is, or has been, a pupil, student/service user or is a member of their family;
5. If you wish to keep in contact with any child or young person under the age of 18, or their family, who has been a user of your service, ensure that you only use work emails or telephone numbers to communicate with them and that your Manager is aware of the contact;

6. If there is any incident, related to this guidance, which involves a child, young person or their family, that causes you concern, report it immediately to your Line manager. Document it as soon as possible, according to your workplace procedures;
7. Ensure you adhere rigidly to the Online Safety policy and Staff Acceptable Use Policy of your workplace. If you breach any part of the AUP, report it immediately as per your workplace procedures;
8. Do not access any illegal or inappropriate websites on your personal computer/laptop or mobile phone. This includes illegal or inappropriate images of children, certain other types of pornography or extremist websites. It is illegal to access or download material that promotes or depicts criminal behaviour;
9. Be very careful when liaising with others online (for example in social networks or using social media). Remember these are not private areas even though you may have privacy settings applied so likes, comments or complaints may be seen by others. Avoid inappropriate communication with individuals under 18, or with who you may be in a position of trust;
10. Use your common sense and professional judgement and expertise at all times to avoid circumstances which are, or could be, perceived to be of an inappropriate nature or which could bring your organisation into disrepute. This relates particularly to social networking sites, social media and mobile phone technology;
11. Remember, digital technology and social media may be the virtual world, but it has an impact on our real world online actions can have offline consequences.