



Ranskill Primary School

Online Safety Policy



Management log

Version	Date authored	Author	Date approved	Date issued	Comments
V1	28 March 2022	Emil	October 3 rd 2022	October 10 th 2022	To continue to secure the protocols to support online safety

Document

Online safety

Author

Alex Steadman

Person responsible for the policy Executive Headteacher

Date approved Summer 2026

Date issued Summer 2026

Review period

Biennially

Next review

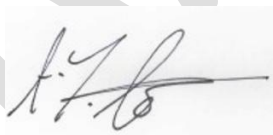
Summer 2028

Reviewer

Alex Steadman

Signed

Signed



Chair of the LGB

Headteacher

DRAFT

Contents

1. Equality	4
2. Introduction	4
3. Roles and responsibilities	5
4. Teaching and learning	6
5. Managing Internet access	6
7. Managing mobile phones and personal devices	8
8. Policy decisions	9
9. Online bullying	9
10. Radicalisation and extremism online	10
11. Indecent images	10

1. Equality

1.1 SHINE Multi Academy Trust (SHINE) and its academies are committed to promoting equal opportunities and all stakeholders¹ will receive equal treatment regardless of age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation (protected characteristics).

2. Introduction

2.1 Online safety encompasses Internet technologies and electronic communications. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

¹ SHINE defines stakeholders as anyone who is invested in the welfare and success of SHINE and its pupils, including premises staff, administrators, teachers, support staff, pupils, parents/carers, families, community members, businesses, and elected officials such as school board members, city councillors, and state representatives.

Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of computing within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Internet – World Wide Web
- online gaming (Xbox, playstation, tablets etc)
- e-mail
- instant messaging (such as Instant Messenger)
- web based voice and video calling (for example, Skype)
- online chat rooms (including Teams)
- online discussion forums
- social networking sites (such as Facebook)
- blogs and Micro-blogs (for example, Twitter)
- podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- video broadcasting sites (such as You Tube)
- music and video downloading (for example, iTunes)
- mobile phones with camera and video functionality

3. Roles and responsibilities

3.1 As online safety is an important aspect of strategic leadership within the school, the headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

3.2 The named online safety leader in our school is the Head of School. It is the role of the online safety leader to keep abreast of current issues and guidance.

3.2 All staff are responsible for promoting and supporting safe behaviours in their classrooms and following school online safety procedures.

3.3 Pupils are expected to take an active part in lessons and activities to support their understanding and confidence in dealing with online safety issues, both at home and school.

3.4 Parents are given information about online safety through the school website and newsletters and are asked to support the school with online safety at home.

4. Teaching and learning

4.1 The purpose of Internet use in school is to raise educational standards, promote pupil achievement, support the professional work of staff and enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

4.2 Internet use benefits education by providing:

- access to world-wide educational resources including museums and art google maps educational and cultural exchanges between pupils world-wide
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across networks of schools, support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- access to learning wherever and whenever convenient

4.3 Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. The school will provide opportunities within a range of curriculum areas to teach online safety, including computing and PSHEE. Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.

4.4 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5. Managing Internet access

5.1 Information systems security will be maintained by

- virus protection being updated regularly

- the security of the school information systems and users will be reviewed regularly
- the school Internet access will be designed to enhance and extend education

5.2 Pupils may only use approved e-mail accounts. They must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from a trusted adult.

5.3 The contact details on the website should be the school address, email and telephone number.

Staff or pupils' personal information must not be published. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright. Pupils' full names are not to be used anywhere on the website without written permission of the parent/carer. Full names will not appear with photographs.

5.4 Images that include pupils will be selected carefully and will not provide material that could be reused.

5.5 Written permission from parents or carers will be obtained before images of pupils are electronically published and consent forms will be stored in pupil files for reference.

5.6 The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends, specific interests and clubs etc. The school will block / filter access to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

5.7 Staff will have access to the school website, where they will be able to update sections relating to their class or subject area. The online safety leader will have administration rights to monitor web pages and users. Staff need to remember that any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content. Full names of pupils will not appear on the website.

5.8 The school will work with their appointed Internet Service Provider to ensure systems to protect pupils are reviewed and improved. The school's broadband access will include filtering appropriate to the age and maturity of pupils. All users will be informed that network and Internet use will be monitored. If staff or pupils discover unsuitable sites, the URL must be reported to the online safety leader, who will then contact the internet provider. Any

material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

5.9 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The use of portable media such as memory sticks and CD ROMS are potential sources of computer virus and staff will be mindful of their use.

5.10 Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

7. Managing mobile phones and personal devices

7.1 The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the discipline/behaviour policy.

7.2 The use of mobile phones and other personal devices by staff in school is covered in the acceptable use of IT policy. If a member of staff breaches the acceptable use of IT policy, then disciplinary action may be taken. Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school will be sent to the school office and kept there until the end of the day.

7.3 Staff may, at times, may communicate with parents via ClassDojo, using their personal devices. It is essential that staff members use their integrity and any images or recordings of pupils or their work are deleted promptly from the personal device and any linked 'clouds'. Personal devices that are used in this way will be monitored frequently during staff meetings to ensure any images or recordings have been deleted. Staff are aware of The Teacher Standards and the Staff Code of Conduct and are aware that improper use, or storage, of images or recordings could lead to disciplinary action.

7.4 Staff are not permitted to use their own personal phones or devices for contacting families within the setting unless in a professional capacity. This may involve some limited communication with parents regarding their child, when it is deemed necessary. Staff are expected to behave in a professional manner and are aware of The Teacher Standards and the Staff Code of Conduct and improper communication may lead to disciplinary action.

7.5 Staff will not make or receive calls on mobile devices, during teaching time, without first seeking permission from the Head of School. This will be for urgent or time-sensitive matters only.

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

8. Policy decisions

8.1 The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications. All staff must read and sign the 'acceptable use of IT policy' before using any school IT resource.

8.2 Parents/carers will be asked to sign and return a consent form for pupil access. Parents will be informed that pupils will be provided with supervised Internet access. Online safety rules will also be displayed clearly in all classrooms.

8.3 Methods to identify, assess and minimise risks will be reviewed regularly. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the broadband provider can accept liability for the material accessed, or any consequences resulting from Internet use.

8.4 The online safety leader will record all reported incidents and actions taken in the online safety incident log and in any other relevant areas. For example, anti-bullying or safeguarding chronology.

8.5 The school will inform parents/carers of any incidents of concerns as and when required.

8.6 The school will manage online safety incidents in accordance with the behaviour policy where appropriate.

8.7 Complaints of Internet misuse will be dealt with under the complaints procedure.

8.8 Any complaint about staff misuse must be referred to the headteacher. Any issues (including sanctions) will be dealt with according to the data protection, disciplinary and child protection procedures. All online safety complaints and incidents will be recorded by the school and in the knowledge of the SHINE data protection officer— including any actions taken.

9. Online bullying

9.1 While online bullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or MSN, are becoming more frequent. As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding

for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of online bullying.

9.2 All incidents of online bullying reported to the school will be recorded. Online bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying. Complaints of online bullying will be dealt with by the Senior Leadership Team. Parents and pupils will need to work in partnership with staff to resolve issues. Any complaint about staff misuse must be referred to the headteacher.

0. Radicalisation and extremism online

10.1 We recognise that children / young people can be enticed into radicalisation as they are more vulnerable and susceptible to this. They therefore can be drawn into violence or they can be exposed to the messages of extremist groups by many means especially on line and through social media. The school recognise that social media is increasingly a child's or young person preferred method of communication which can increase their risk to exposure to radicalisation.

10.2 We will try and help our pupils to keep safe on line and consider the impact of social media networking sites with additional consideration to the threat of exposure to extremism and radicalisation. We are aware of the increased risk of online radicalisation and how terrorist groups seek to radicalise young people on line.

10.3 We will treat any worry or concern that a child or young person in the school may be exposed to possible extremism, extremist ideology and or radicalisation as a Prevent concern. We will use the guidance and assessment as prescribed by SHINE.

11. Indecent images

11.1 We recognise that this is an increasing safeguarding concern which requires a robust response. We will seek advice from agencies and professionals acknowledging that there are both national and local guidance that we need to adhere to in order to tackle the concerns and work in partnership with our agencies.

11.2 We will refer to:

- SHINE's child protection and safeguarding policy <https://www.shine-mat.com/pupil-welfare/>
- <http://www.workingtogetheronline.co.uk/>
- The DfE guidance 2018 on Searching Screening and Confiscation Advice

- <https://assets.publishing.service.gov.uk/government>

12 Communicating the policy

12.1 Online safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers and the school will provide opportunities within a range of curriculum areas to teach online safety. Pupils will also be involved

Page

in the annual 'Safer Internet Day' which takes place in February. Members of the school council will look through this policy and recommend any necessary amendments.

12.2 To protect all staff and pupils, the school will implement acceptable use policies.

12.3 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff training in safe and responsible Internet use both professionally and personally will be provided every two years with a reminder during the safeguarding update every year. All staff are 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. All staff will be given a copy of this policy.

12.4 Parents/carers' attention will be drawn to the importance of online safety through newsletters home, the school website, internet safety assembly and information home.

Guidance for parents on online safety will be made available to parents in a variety of formats. Parents/carers will be asked to sign permission slips about the children's use of their child's name, photo and work being used on the school website, the media and twitter.

12.4 The school website contains useful information and links to sites like Thinkuknow, CEOP and the NOS Webpage.

12.5 We will make this policy available to our parents/carers, to our local community. This Policy will also be made available on the school website.

Page