Online-Safety Policy

March 2023

Our Online Safety Policy will operate in conjunction with other policies including those for Right Respecting Schools, pupil behaviour, anti-bullying, curriculum, data protection and security.

It involves all members of staff from the Headteacher to any new members of staff. Through its compliance, it will ensure that everyone knows and understands their responsibilities and can act upon them.

March 2023

Lydgate Junior School Online-Safety Policy

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 and provides safeguards and awareness for users to enable them to control their online experiences.

Lydgate Junior School is working towards Gold award as a Rights Respecting School. To do this we put the 54 Articles of the UN Convention on the Rights of the Child at the forefront of all our thinking and actions. The school's online-safety policy will operate in conjunction with other policies also including those for Pupil Behaviour, Curriculum, Data Protection and Security.

The curriculum statement on Lydgate Junior School Website outlines our Vision Statement for Online-Safety.

The Online-Safety Policy will be reviewed annually. This policy will be reviewed again in January 2024.

Online Safety at Lydgate Junior School: Vision Statement

INTENT: Our online safety education empowers pupils to think critically, behave safely and participate respectfully in our digital world. It is our intention that the children should be mindful of their own well-being when using social media and how to be safe when using digital technology. They will develop an understanding of what is acceptable and unacceptable behaviour online, and how to report their concerns. We will encourage a participation in the wider community and demonstrate how, through network technologies, this can bring communities closer together.

The internet allows people to improve the quality of their lives, therefore we aspire to help children to become confident and respectful users of modern technology, ready to equip them in all aspects of their lifelong learning and enjoyment.

IMPLEMENTATION: The most effective approach to online safety is to treat it as a whole school community, with educational messages embedded across Computing/ICT, PSHE, RHE and citizenship, as well as touching on online safety issues across the curriculum whenever it is appropriate.

At Lydgate Junior School, we have developed a bespoke and informative ICT and online safety curriculum based on the progressive frameworks provided by eLearning Sheffield for Computing and RHE.

During their time at Lydgate Juniors School, children cover several units re-visiting each area and embedding the language of the subject. The online safety curriculum is progressive and children build on the skills and understanding gained in prior years.

Children have weekly timetabled access to the ICT suite but also access to mobile technology including laptops and iPads. In addition, they have access to a range of physical programming devices to develop their understanding of how their safe searching skills can be adapted for practical purposes. We also celebrate and promote ‘Safer Internet Day’ during February each year.

As pupil voice is an important part of our RRS School, pupils complete questionnaires to evaluate their understanding of online safety so that we regularly monitor the effectiveness of our curriculum so that we can plan for, and support, the ever-changing demands in technology and our pupils’ safe relationship with technologies and the online world.

IMPACT: At Lydgate Junior School, online safety is embedded across the curriculum to provide relevant opportunities for approaching a range of key online safety issues such as cyberbullying, safe social networking, healthy digital behaviours, sexting, privacy and online reputation.

After the implementation of our online safety curriculum, children at Lydgate Junior School will become confident digital citizens. They will have the skills and knowledge to use technology responsibly and safely, and be aware of the consequences of their online activity.

How can Internet Use Enhance Learning?

- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The internet will be used to provide access to pictures, videos, audio effects, games, stimulation, replay, use for examples and prompts… as staff and pupils benefit from its wealth of resources.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the Local Authority helpdesk via the online-safety coordinator.
- School will ensure that the use of internet-derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The School's Rules for using the internet are clearly displayed around school (see Appendices B & C).

Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- Our school blocks / filters access to social networking sites and newsgroups unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space.
- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

- Pupils are encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with Blue Box schools technical support.
Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided and filtered and monitored by **Smoothwall,** this system alerts the DSL and the Deputy DSL if there is a concern.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Video Conferencing

The Staff at Lydgate Junior School consider the following seven tips to help protect educational Zoom calls:

1. **Lockdown the meeting room by using passwords and requiring authentication.** That way, only people you want are on the call. Remove unwanted or disruptive participants.
2. **Lockdown screen sharing.** That way, only people you want can share their screen.
3. **Be careful about clicking on links and opening documents sent to you**. Verify via another communication channel that the sender really did send the link or document to you.
4. **Be careful what you show in the background**. For example, move any personal items or photographs of your children out of shot if you do not want those to be seen. Zoom also offers the chance to change the background behind you. (Other meeting apps — for example, Skype — give you the option to blur whatever is behind you.)
5. **Be careful what is on your screen before using the screen sharing function**. For example, any other tabs or private chat windows that may be open or any documents that may display sensitive financial or personal information. Be careful about accidentally showing an item of mail with your address on it, or accidental close-ups of your ID, a credit card, or anything else you might not want a stranger to see.
6. **Check your settings.** Some security settings are not enabled by default. Zoom has different settings for desktop and mobile — the desktop settings are more detailed and offer more control than the cell phone version. For example, hosts have more management tools, and users can only manage blocked accounts on desktop.
7. **Keep an eye on news about app updates.** Keeping up to date will give you a better idea of the various privacy and security features which are available.

(Advice from https://www.kaspersky.co.uk/resource-center/threats/video-conferencing-security-how-to-stay-safe)

Parents support their children at home with home-school learning activities and are aware of the 'Positive Behaviour Policy.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Ordinarily, mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden under the behaviour policy.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff, Governors or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate, appropriate and as up to date as reasonably possible.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Parents will be informed in our prospectus that that we may use photos of children on our website. Parents and Carers will be able to withhold their permission.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the Freedom of Information Act 2000.

IMPACT:

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Sheffield City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the online-safety policy is adequate and that the implementation of the online-safety policy is appropriate.

Handling Online-safety Complaints (*See Appendix A.)*

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School Online-Safety Policy and its importance will be explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff use of social media websites may be subject to the professional standards and code of conduct.

Parents

Parents' attention will be drawn to the School Online-Safety Policy in newsletters and on the school Web site along with other Online-Safety guidance.

Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online-safety is therefore an essential part of the school's online-safety provision. Children and young people need the help and support of the school to recognise and avoid online-safety risks and build their resilience.

Online-safety education is provided in the following ways;

- Teachers deliver a series of specific online-safety related lessons in every year group as part of the ICT and RSHE/PSHE/RRS curriculums. Online-safety is also delivered throughout other cross-curricular topics whenever it is necessary and relevant.
- We celebrate and promote Online-safety through a planned program of assemblies and whole school activities, including promoting Safer Internet Day in February each year.
- We discuss, remind and raise relevant Online-safety messages with pupils routinely wherever possible opportunities arise 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 is carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils are taught how to use a range of age appropriate online tools in a safe and effective way.
- Staff model safe and responsible behaviour in their own use of technology during lessons.
- We teach pupils how to search for information and to evaluate the content of websites when using them in any curriculum area.
- When searching the internet for information, pupils are guided to use age-appropriate search engines. All use is monitored and pupils are guided as to what to do if they come across unsuitable content.
- All pupils are taught in an age appropriate way about copyright in relation to online resources and are taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils are taught about the impact of cyber-bullying and know how to seek help if they affected by any form of online bullying.
- Pupils are 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.

Support for Staff / Parents

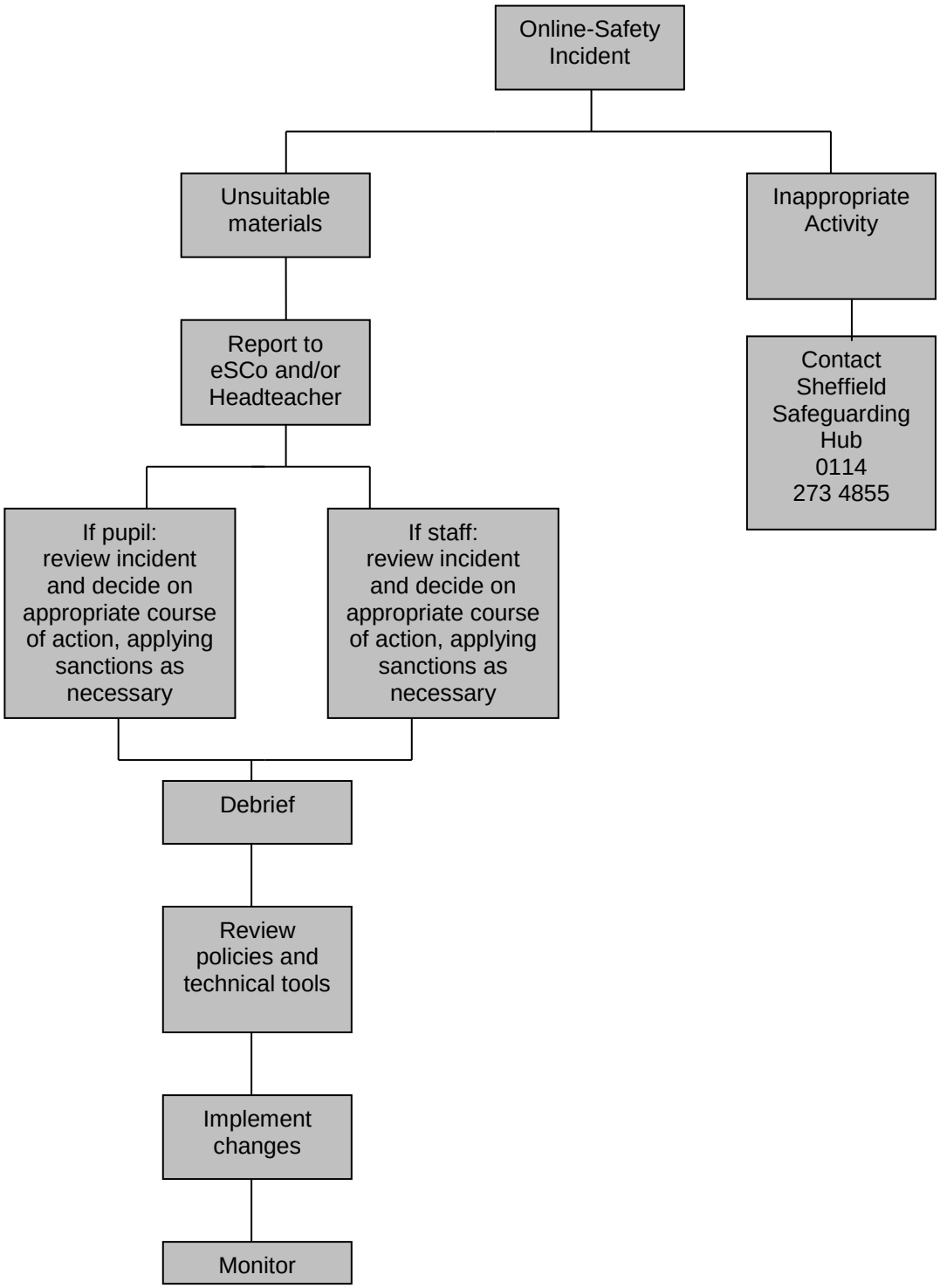
It is essential that all staff receive online-safety training and understand their responsibilities, as outlined in this policy. The Headteacher and Online-Safety co-ordinator provide advice, guidance and training as required.
The school website is also regularly updated with relevant flyers and support information for pupils, staff and parents.
The School also supports the Safer Internet Day within the Spring Term to promote awareness of the importance of Online-Safety for all.

APPENDICES:

- **Referral Process – Appendix A**
- **Online-Safety Rules – Appendix B**
- **Online-Safety Audit – Appendix C**
- **Staff Acceptable Use Policy, Staff Information Code of Conduct – Appendix D**

Referral Process – Appendix A

Flowchart for responding to e-safety incidents in school



Online-Safety Rules Posters – Appendix B

Online-Safety Rules

These Online-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Online-Safety Audit – Appendix C

Good Habits

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

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of online-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Yorkshire and Humberside Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

Online-Safety Audit – Primary Schools

This quick self-audit will help the senior management team (SMT) assess whether the online-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	**Yes** /N
Date of latest update:	March 2022
The Policy was agreed by governors on: (JW meeting governors June 2022) ……	
The Policy is available for staff at:	through school server/intranet
And for parents at:	https://www.lydgatejunior.co.uk/
The Designated Safeguarding Lead is:	Rachel Hurding
The Online-Safety Coordinator is: Lead: Rachel Hurding Teacher: Joanne Watkinson	
Has online-safety training been provided for both pupils and staff?	**Yes** /N
Is the Think U Know training being considered?	**Yes** /N
Do all staff sign an ICT Code of Conduct on appointment?	**Yes** /N
Do parents sign and return an agreement that their child will comply with the School online-Safety Rules?	**Yes** /N
Have school online-Safety Rules been set for pupils?	**Yes** /N
Are these Rules displayed in all rooms with computers?	**Yes** /N
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	**Yes** /N
Has the school filtering policy has been approved by SMT?	**Yes** /N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Yes** /N

Staff Acceptable Internet Use Policy – Appendix D

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to read and abide by this Code of Conduct. Staff should consult the school's online-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school online-Safety Coordinator or the Designated Safeguarding Lead.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote online-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

If I disagree with this code of conduct or other aspects of this Online-Safety Policy, then I will discuss my concerns with the Online-Safety Co-ordinators Joanne Watkinson and / or the Headteacher, Rachel Hurding.