E-Safety Policy

Park Spring Primary School

Approved by:	C.Shaw	**Date:**	Spring 2023
Last reviewed on:	Spring 2023		
Next review due by:	Spring 2024		

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for computing, anti-bullying and child protection.

- The school has an e safety coordinator; **Callum Shaw,** who will work with Child Protection designated staff: **Rachel Horan** (Head Teacher) **Claire Thorson** (Senco), **Wendy Holl** (Family Liaison), **Kath Doran** (inclusion team).
- Our e-Safety Policy has been written by the school, building on the Leeds e-Safety Policy and government guidance. It has been agreed by all staff and approved by governors and the PTA (FOPs).

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is currently provided by EXA NETWORKS.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content

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

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- The school has two separate servers, the admin (office) and curriculum (rest of school). These are connected now but staff will only be able to access SIMs as well as their own content.
- The head teacher is the only person to be able to access both networks from one computer.
- The school has a wireless network which links with the curriculum server.

Wireless Network

- The schools wireless network is secure. There is a password which only the computing subject leader and ICT technician know.
- Pupil devices (iPads and laptops provided by school) are already set up on the network.
- Staff are advised to contact the computing leader when accessing with personal equipment.
- It will be managed by the computing subject leader / e-safety coordinator and ICT technicians.

E-mail

- Following COVID-19, each pupil has an Office 365 account. At present, children are able to use the provided email accounts, however, can only email people within the school group (Staff and other pupils.)
- 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.
- E-mail sent to an external organisation 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.

Published content and the school web site/Facebook

- The contact details on the Web site/Facebook should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher, **Rachel Horan**, and computing subject leader, **Callum Shaw**, plus **the Communication Team (Vicky Benson, Nichola Horner, Kate Beverly and Amy Smith)** will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Only pupils' forenames will be used on the Web site or Facebook, especially in association with photographs.
- Pupil's work can only be published with the permission of the parents (List of non-authorised children has been created for every year group).
- All parents / carers will need to give consent before their child(ren)s photographs or videos will appear on the website/Facebook.

Social networking and personal publishing

- EXA NETWORKS will block/filter access to social networking sites.
- Sites will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. This is delivered through the curriculum's **Digital Citizenship** module and supported at home through access to **The National Online Safety Hub**.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and as part of staff training on online safety.

Managing filtering

- The school will work with the Quantum (through exa-networks) to ensure systems to protect pupils are reviewed and improved. Quantum can be accessed by **Callum Shaw** and **SchoolsICT**.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator, **Callum Shaw**, who will look into it and add into the restricted section on Quantum.

Managing videoconferencing

- Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils or parents is required. If a phone is unavailable (for example, the staff member is working from home), the private number must be blocked before dialling.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Leeds City Council can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety coordinator **Callum Shaw,** and a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher

  Mrs R. Horan.
- 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.
- **Appendix 2 details the response to a potential online incident.**

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying (see appendix 1) and this will be in accordance with the schools anti-bullying policy.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored.
- Pupils are taught a Digital Citizenship lesson every half term. The topic of these varies by year group. Further information available from the Computing Subject leader **Callum Shaw**.
- In addition, pupils will have an **Online Safety Day**, using UK Safer Internet resources linked with **National Online Safety** resources and are tailored each year by the safety coordinator, **Callum Shaw.**

Staff and the e-Safety policy

- All staff will be given access to the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Parents have also been provided a link to sign up to the **National Online Safety Hub.**

Addendum 1 – Taken from SAFEGUARDING & CHILD PROTECTION POLICY FOR SCHOOLS & COLLEGES Addendum COVID-19 school closure arrangements for Safeguarding and Child Protection at Park Spring Primary School.

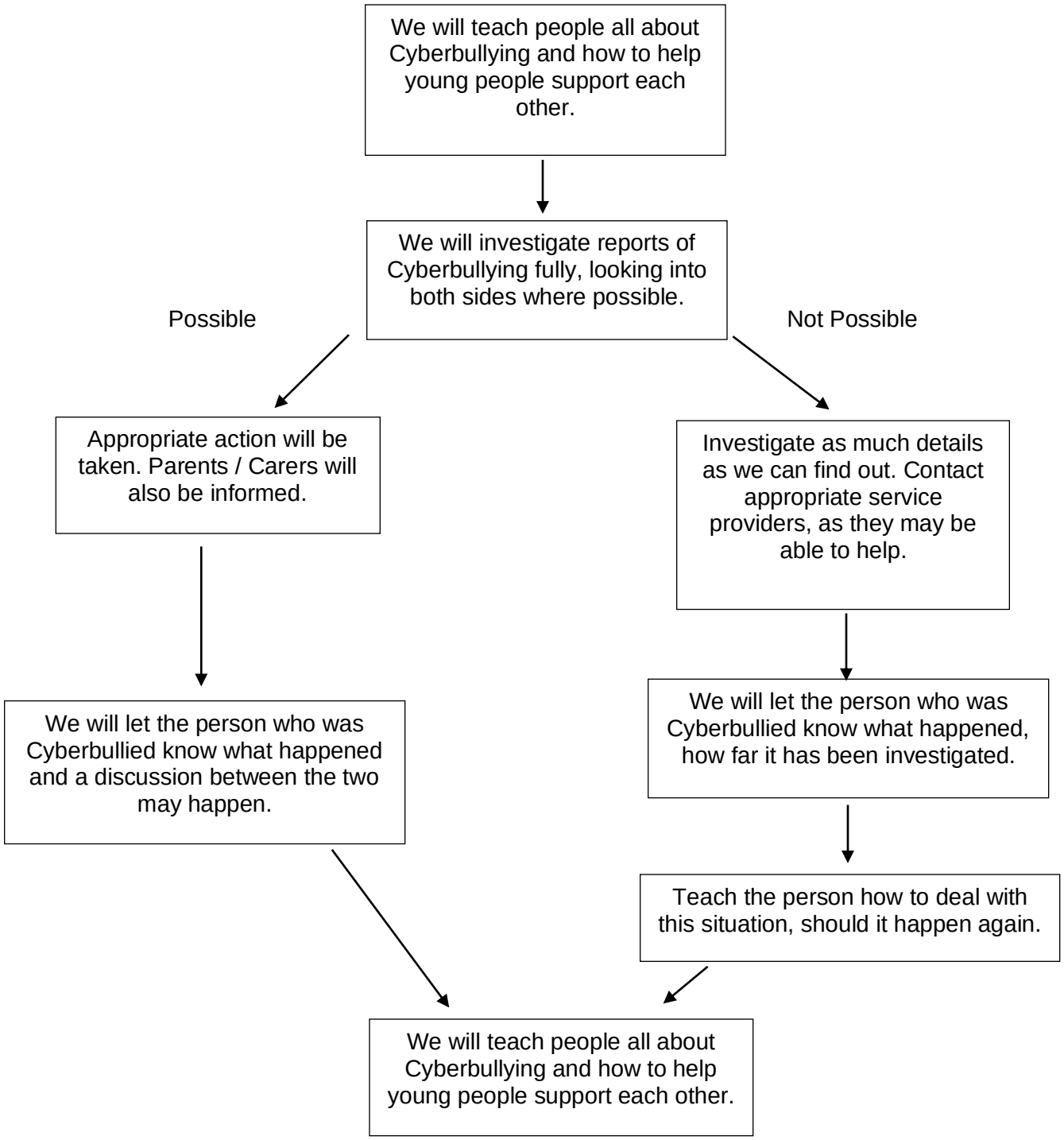
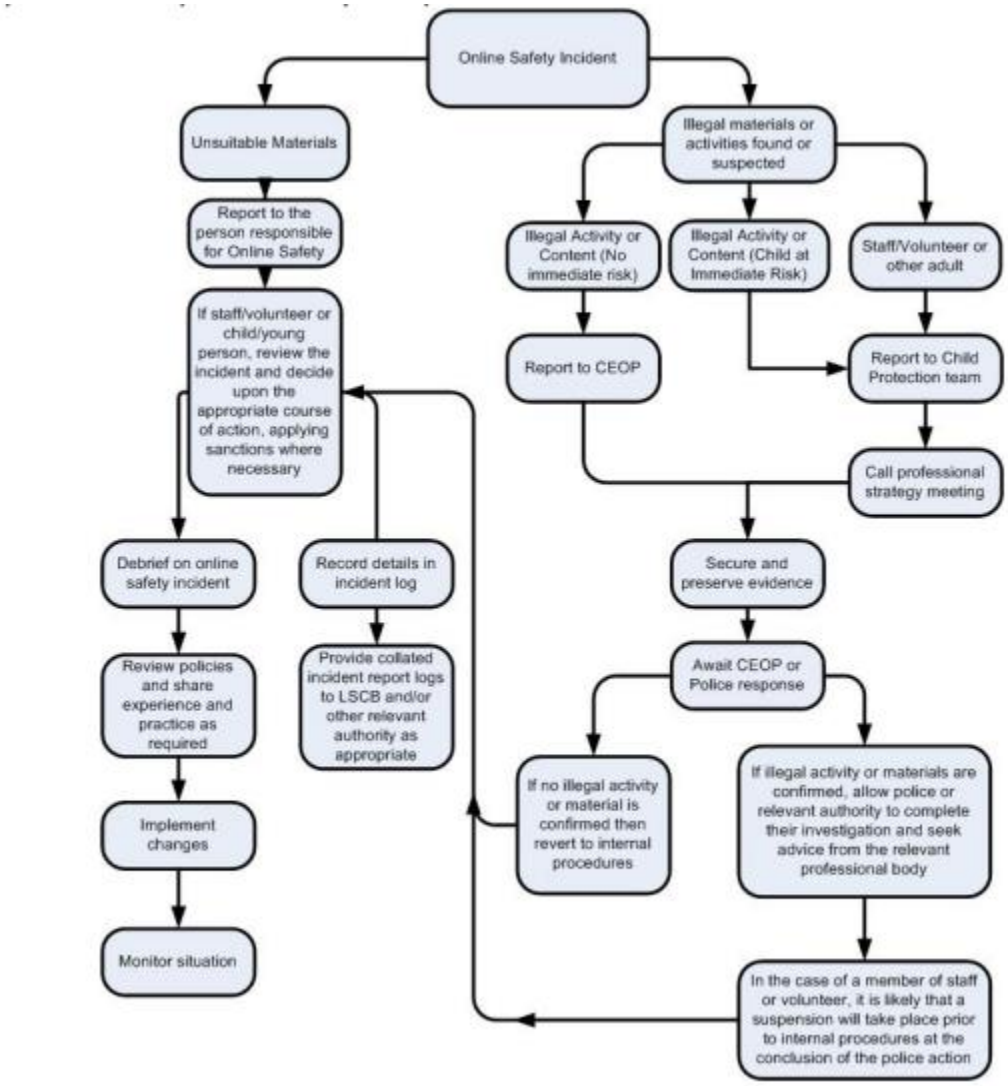
The following has been taken from the addendum. It has been updated slightly, to reflect the delivery of live lessons, which previously were not being taught.

Children and online safety away from school

- It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.
- Online teaching should follow the same principles as set out in the Guidance for safer working practice for those working with children and young people in education settings (National Safer Recruitment Consortium May 2019).
- Park Spring Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.
- Park Spring Primary School staff may choose to deliver live classes during lockdown. Short video recordings may be produced and published on the school website for children and parents to view e.g. reading a story. A range of platforms may be used to engage children in these, including Microsoft Teams, Zoom and Tapestry.
- Below are some things to consider when delivering virtual lessons, especially where webcams are involved:
    - No 1:1s, groups only. In cases where 1:1 tuition is essential, staff must seek formal written agreement from a senior manager and the pupil's parent.
    - Staff and children must wear suitable clothing, as should anyone else in the household.
    - Any computers used should be in appropriate areas, for example, not in bedrooms; staff need to be mindful that backgrounds do not compromise personal confidentiality or breach the guiding principles of safer working practice guidance for staff working in educational settings.
    - The live class will be recorded where possible, so that if any issues were to arise, the video can be reviewed.
    - Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
    - Language must be professional and appropriate, including any family members in the background.
    - Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils.
    - Staff should record, the length, time, date and attendance of any sessions held

Cyberbullying Appendix 1

Park Spring Primary School has a responsibility for its children's welfare whether they are in school or out of school, especially when it comes to technology. The schools procedures, when it comes to Cyberbullying, reflect the schools Anti-bullying policy when investigating incidents or allegations of Cyberbullying. The following chart shows how the incidents will be investigated.



Appendix 2 – SWGfl e-Safety model.