E-Safety Policy

Park Spring Primary School

Approved by:		**Date:** Spring 2025
Last reviewed on:	Spring 2025	
Next review due by:	Spring 2026	

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; **Victoria Benson,** who will work with Child Protection designated staff: **Rachel Horan** (Head Teacher), **Oliver Woods** (Assistant head and safe guarding lead), **Nils Hansen** (Senco), **Wendy Holl** (Family Liaison officer), **Kath Doran** (Family support worker and behaviour support worker).
- 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).

Roles and responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The head teacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

Details of the school’s designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- ➢ Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- ➢ Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- ➢ Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- ➢ Working with the ICT manager to make sure the appropriate systems and processes are in place
- ➢ Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- ➢ Managing all online safety issues and incidents in line with the school’s child protection policy
- ➢ Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- ➢ Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- ➢ Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- ➢ Liaising with other agencies and/or external services if necessary
- ➢ Providing regular reports on online safety in school to the headteacher and/or governing board
- ➢ Undertaking annual risk assessments that consider and reflect the risks children face
- ➢ Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- ➢ Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ➢ Ensuring that the school’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- ➢ Conducting a full security check and monitoring the school’s ICT systems on a monthly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems.
- Following the correct procedures by Park Spring if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

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 using Quatumn.
- Monitoring systems are in place and regularly checked so that no child can access harmful content via the school's IT systems and concerns can be spotted quickly.
- 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.
- The school will ensure that they teach their pupils about safeguarding, including online safety.

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.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or the DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Park Spring recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others.

Park Spring will treat any use of AI to bully pupils in line with our anti bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Acceptable use of internet in the school

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement/mobile phone policy.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside of school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- Keeping operating systems up to date by always installing the latest updates

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don’t want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

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 one 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 is not advised that the network is used on personal devices.
- 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.
- 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 Website/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, **Victoria Benson**, plus **Kate Beverley Caroline Slape** and will have editorial responsibility and ensure that content is accurate and appropriate.
- Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.
- The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

Publishing pupil's images and work

- Only pupils' forenames will be used on the Website or Facebook, especially in association with photographs.
- Pupil's work can only be published with the permission of the parents.
- 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

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

- 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 **Victoria Benson** and **Schools ICT**.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator, **Victoria Benson**, who will look into it and add into the restricted section on Quantum.

Passwords

- All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.
- Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
- Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

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.
- 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.

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 **Victoria Benson,** 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

- 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 **Victoria Benson.**
- 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, **Victoria Benson.**
- Pupils should be aware that Internet traffic can be monitored and traced to the individual user.

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.**

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

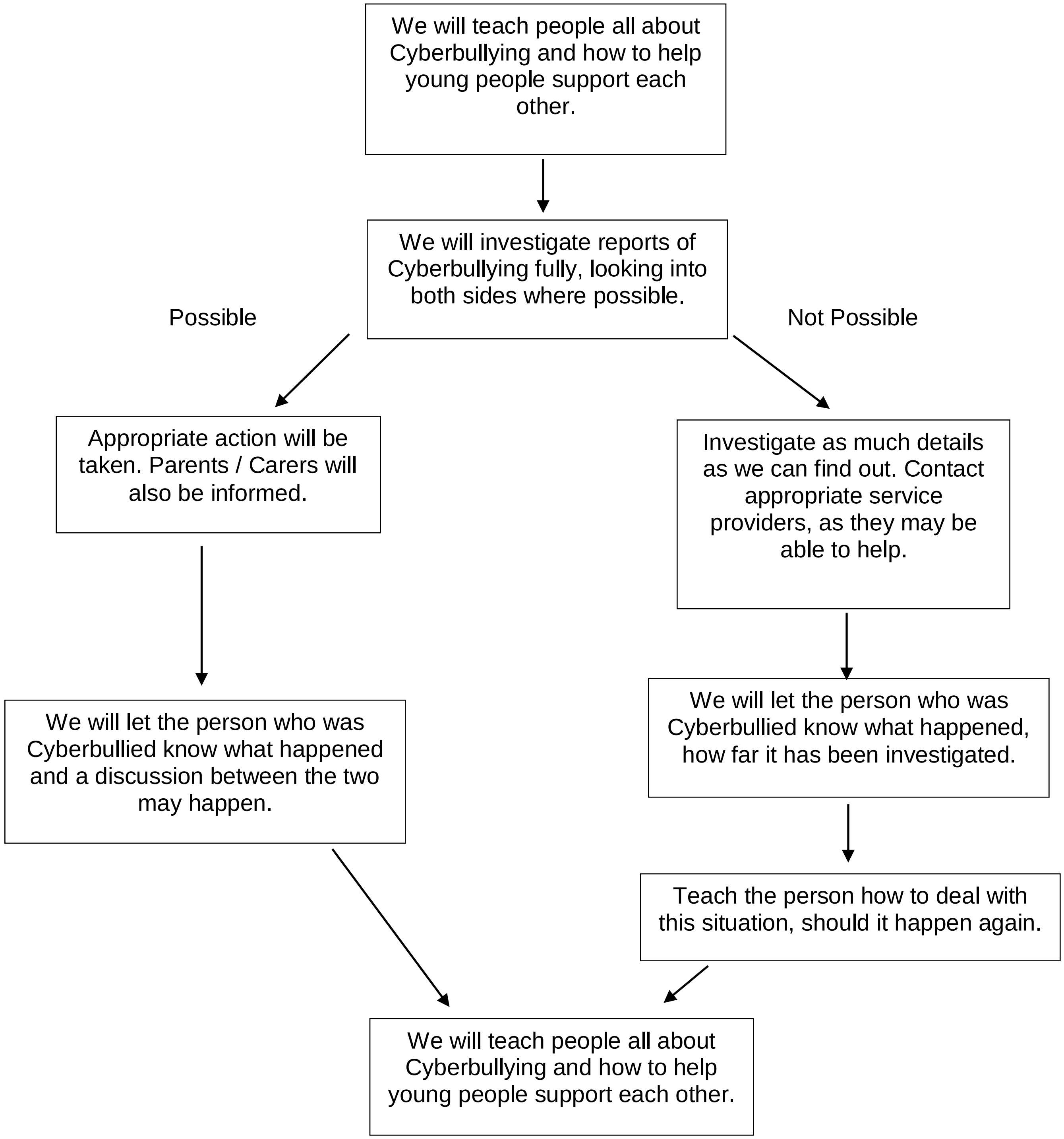
Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

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.



We will teach people all about Cyberbullying and how to help young people support each other.

We will investigate reports of Cyberbullying fully, looking into both sides where possible.

Possible

Not Possible

Appropriate action will be taken. Parents / Carers will also be informed.

Investigate as much details as we can find out. Contact appropriate service providers, as they may be able to help.

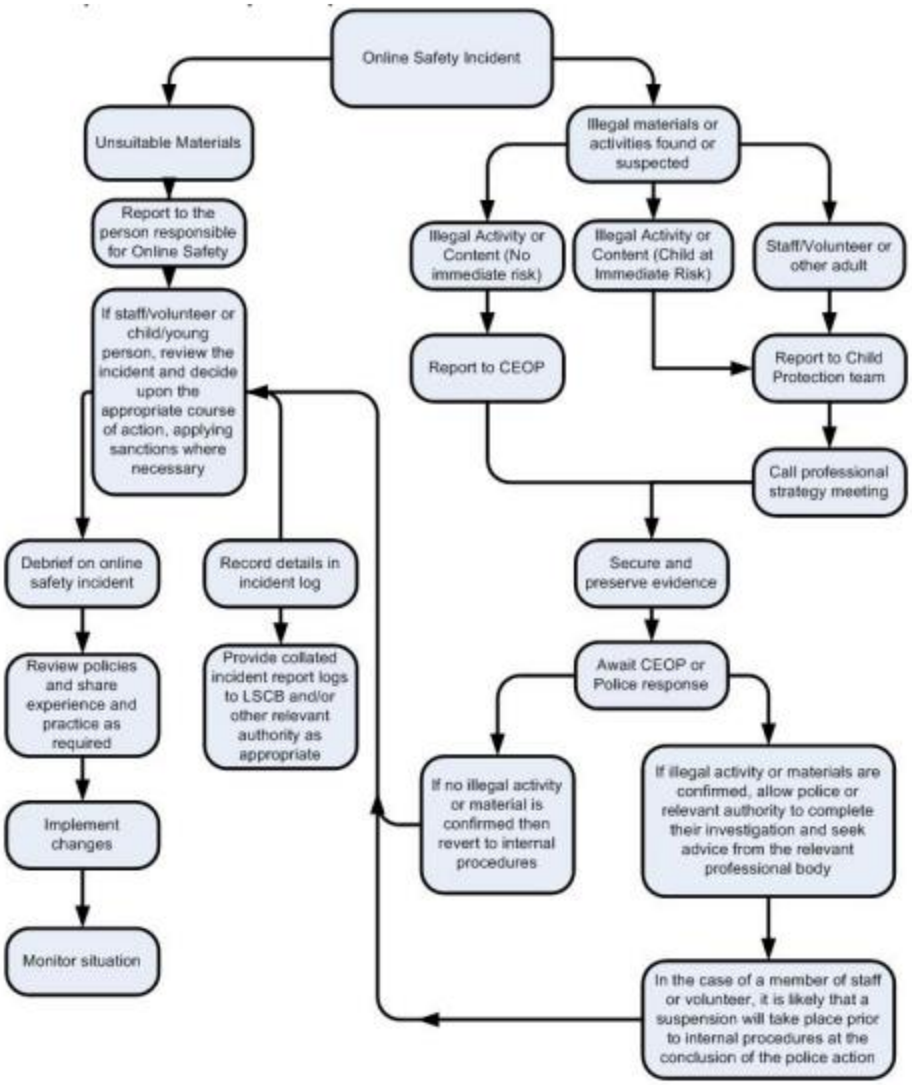
We will let the person who was Cyberbullied know what happened and a discussion between the two may happen.

We will let the person who was Cyberbullied know what happened, how far it has been investigated.

Teach the person how to deal with this situation, should it happen again.

We will teach people all about Cyberbullying and how to help young people support each other.

Appendix 2 – SWGfl e-Safety model.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action