Lingdale Primary School

'Working together to be the best we can be'

E-Safeguarding Policy

Date Written:	Sept 2023
Written by:	Sarah Thornton
Adopted by the Governing Body:	September 2023
Date of Next Review:	Sept 2024

POLICY INTRODUCTION

Digital technologies have become integral to the lives of young people, both within education and outside. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. With the challenges that are the result of the current pandemic, use of digital platforms has become even more integral to learning and with this further measures are needed to keep members of the school community safe. Young people have an entitlement to safe Internet access at all times.

The Lingdale Primary School E-Safeguarding policy encompasses the necessary measures to ensure that risks associated with internet use are carefully managed and reduced, helping all users to be responsible and enabling them to stay safe while accessing the Internet and other communication technologies for educational and personal use.

SCOPE OF POLICY

- This policy applies to all members of the school (including staff, students, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of the School ICT systems, both in and out of the school.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other e-safeguarding incidents covered by this policy, which may take place out of the school, but is linked to membership of the School.
- The Education Act 2011 gives the School the power to confiscate and search the contents of any mobile device if the Head teacher believes it contains any illegal content or material that could be used to bully or harass others.
- The School will, where known, inform parents / carers of incidents of inappropriate e-safeguarding behaviour that take place out of the school.

DEVELOPMENT/MONITORING/REVIEW OF THIS POLICY

This policy has been developed by the E-Safety group made up of:

- Senior Leadership Team
- Teachers
- ICT Technical staff
- Governors
- Parents

SCHEDULE FOR DEVELOPMENT/MONITORING REVIEW

Title	**E-Safeguarding Policy**
Version	3.0
Date	September 2023
Author	Head Safeguarding and E-safety
	Sarah Thornton
This e-safeguarding policy was approved by the Governing Body on*:*	September 2023
Monitoring will take place at regular intervals (at least annually):	Annually

The Governing Body will receive a report on the implementation of the policy including an analysis of any e-safeguarding incidents:	Annually
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2023
Should serious e-safeguarding incidents take place, the following external persons / agencies should be informed:	*Joanne Dickson CPOE Child Protection Officer for Education*

- The school will monitor the impact of the policy using:
- Logs of reported incidents (Forensic Monitoring, SIMS logs)
- Internal monitoring data for network activity (Smoothwall logs, filtering)
- Surveys / questionnaires of:
  - students
  - parents / carers
  - staff

COMMUNICATION OF THE POLICY

The E-Safeguarding Policy will be distributed to staff and governors. It will be available to parents and students on the website. It will be communicated to students through the ICT lessons and assemblies.

- The School's senior leadership team will be responsible for ensuring all members of staff and students are aware of the existence and contents of the E-Safeguarding policy and the use of any new technology.
- The E-Safeguarding policy will be provided to and discussed with all members of staff formally.
- E-Safety training will be part of the transition programme at KS2 – KS3 students' responsibilities regarding the E-Safeguarding policy will be reviewed.
- Pertinent points from the E-Safeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within the School.
- The key messages contained within the E-Safeguarding policy will be reflected and consistent within all acceptable use policies in place within the School.
- The School embeds E-Safeguarding messages across the curriculum whenever the Internet or related technologies are used.
- The E-Safeguarding policy will be introduced to the students at the start of each Academic year.
- Safeguarding posters will be prominently displayed around the School.
- A log of E-Safety training will be kept by the Business manager for Child Protection and E-Safety.

ROLES AND RESPONSIBILITIES

We believe that E-Safeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for teaching and learning.

Responsibilities of the Senior Leadership Team:

- The head teacher has overall responsibility for E-Safeguarding all members of the School community, though they will be supported by the SLT and computing lead within school.
- The Senior Leadership Team are responsible for ensuring that the DSL for Child Protection and E-Safety and other relevant staff receive suitable training to enable them to carry out their E-Safeguarding roles and to train other colleagues when necessary.
- The head teacher and senior leadership team will ensure that there is a mechanism in place (regular line-management meetings) to allow for monitoring and support of those in the School who carry out the internal E-Safeguarding monitoring role.

Responsibilities of the E-Safeguarding Group

- To ensure that the School's E-Safeguarding policy is current and pertinent and is systematically reviewed at agreed time intervals
- To ensure that School Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the School community the safe use of the Internet and any technologies deployed within the School.

Responsibilities of the DSL for Child Protection and E-Safety

- To promote an awareness and commitment to E-Safeguarding throughout the School.
- To be the first point of contact in the School on all E-Safeguarding matters.
- To take day-to-day responsibility for E-Safeguarding within the School and to have a leading role in establishing and reviewing the School's E-Safeguarding policies and procedures.
- To lead the School E-Safeguarding group.
- To communicate regularly with School technical staff and the designated E-Safeguarding governor
- To develop an understanding of current E-Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in E-Safeguarding issues.
- To ensure that E-Safeguarding education is embedded across the curriculum.
- To ensure that E-Safeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board, the NGfl and other relevant agencies as appropriate.
- To monitor and report on E-Safeguarding issues to the E-Safeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safeguarding incident.
- To ensure that an E-Safeguarding incident log is kept up to date.

Responsibilities of the Teaching and Support Staff:

- To read, understand and help promote the School's safeguarding policies and guidance.
- To read, understand and adhere to the School staff Acceptable Use Policy.
- To report any suspected misuse or problem to the DSL for Child Protection and E-Safety.
- To report any incidents of sexting (where young people share youth produced sexual imagery and includes both photos and videos) to the Designated Safeguarding Lead (DSL) for investigation and appropriate follow up. Staff should not view these images.
- To develop and maintain an awareness of current safeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with students should be on a professional level and only through School based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide students carefully when engaged in learning activities involving technology.
- To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms which exist within the School.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

Protecting the professional identify of all staff, work placement students, guests and volunteers

Communication between adults and children / young people, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums, blogs etc.

When using digital communications, staff and volunteers should:

- Only make contact with young people for professional reasons and in accordance with the policies and professional guidance of the School.
- Not share any personal information with a young person e.g. should not give their personal contact details to young people including e-mail, home or mobile telephone numbers.
- Not request, or respond to, any personal information from the young person, other than that which might be appropriate as part of their professional role, or if the young person is at immediate risk of harm.
- Not send or accept a friend request from the young person on social networks.

- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with young people so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with young people in their care (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the school into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Child Protection Officers:

- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of Students:

- To read, understand and adhere to the School's student Acceptable Usage Policy.
- To help and support the School in the creation of e-Safeguarding policies and practices and to adhere to any policies and practices the School creates.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in the School and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in the School and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within the School.
- To discuss e-Safeguarding issues with family and friends in an open and honest way.
- In the event of remote learning, understand that Google Classroom can only be used using their school log in details and no personal information should be shared.
- Use video technology related to remote learning in a neutral environment and not their own personal areas (i.e. bedroom)

Responsibilities of Parents / Carers:

- To help and support the School in promoting E-Safeguarding.
- To read, understand and promote the School's Student ICT Acceptable Usage Policy with their children before signing it themselves.
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies that their children use in the School and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss E-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology
- To consult with the school if they have any concerns about their children's use of technology.
- Enable children to use technology provided by the school in a safe and neutral environment.

To sign a home-school agreement containing the following statements:

- We will support the school approach to online-Safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community.
- We will support the School's stance on the use of ICT and ICT equipment.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- Parents and carers are asked to read through and sign the Student ICT Acceptable Usage Policy on behalf of their children on admission to the school.

Responsibilities of the Governing Body:

- To read, understand, contribute to and help promote the school's E-Safeguarding policies and guidance.
- To develop an overview of the benefits and risks of the Internet and common technologies used by students.
- To develop an overview of how the school's ICT infrastructure provides safe access to the Internet.

- To develop an overview of how the school encourages students to adopt safe and responsible behaviours in their use of technology, in and outside of the school.
- To support the work of the E-Safeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its E-Safeguarding strategy.

The role of the E-Safety Governor includes:

- regular meetings with the DSL for Child Protection and E-Safety
- reporting to Governors meeting

Education - Students

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

E-Safety education will be provided in the following ways:

- We will provide a series of specific E-Safeguarding-related lessons in specific year groups as part of the computing curriculum.
- We will celebrate and promote E-Safeguarding through a planned programme of assemblies (when possible to do so) and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant E-Safeguarding messages with students routinely wherever suitable opportunities arise during 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 will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind students about their responsibilities through the Student ICT Acceptable Use Policy.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach students how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the Internet for information, search engines will be set to 'Safe Search' so that only appropriate content is accessed. All use will be monitored and students will be reminded of what to do, if they come across unsuitable content.
- Students will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students will be 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.

All of the above supports the areas of the computing curriculum in each phase of education:

In **Key Stage 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.

In **Key Stage 2**, pupils 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 pretending to be someone they are not.
- The same principles apply to online relationships as it does 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 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.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

All staff (including Governors)

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and ICT Acceptable Usage Policies.
- This E-Safeguarding policy and its updates will be presented to and discussed by staff in staff and team meetings
- The E-Safety Group will provide advice / guidance / training to individuals as required.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way and in promoting the positive use of the Internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents understand these issues through:

- parents' evenings
- newsletters
- letters
- information about national / local e-safety campaigns / literature

CYBER BULLYING

Cyber bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

PREVENTING CYBER BULLYING

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Anti Bullying Policy.

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the Internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals, in the short or longer term. There are many reported incidents of employers carrying out Internet searches for information about potential and existing employees.

The School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others, without their permission.
- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained in the ICT agreement before photographs of students are published on the School website or elsewhere.
- Student's work can only be published with the permission of the student and parents or carers.
- When searching for images, video or sound clips, students will be taught about copyright and acknowledging ownership.

MANAGING ICT SYSTEMS AND ACCESS

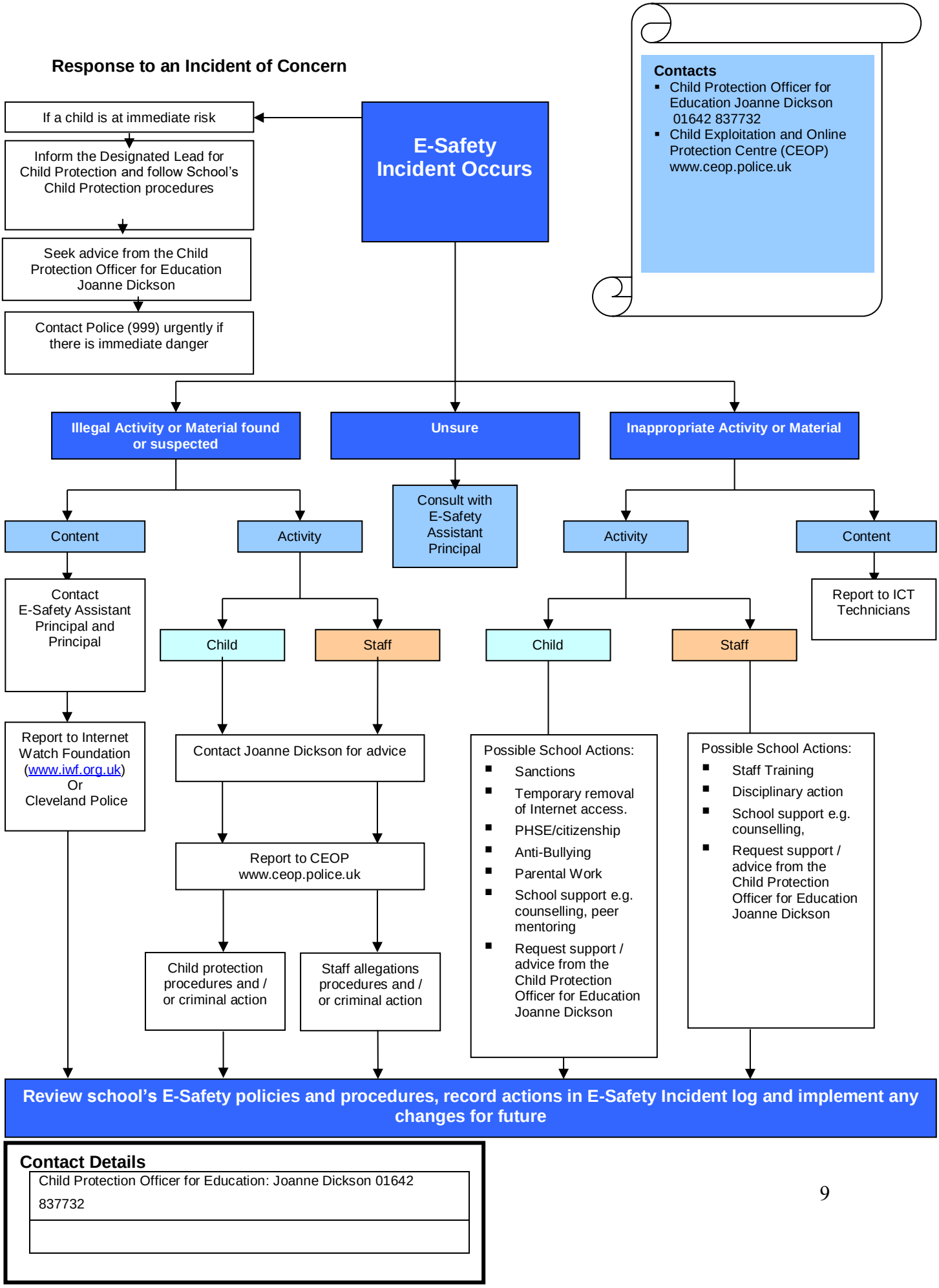
- The School will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as required.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have Internet access and the appropriate level of access and supervision they should receive.
- Members of staff will access the Internet using an individual username and password, which they will keep secure. They will ensure that they log out, or lock the computer after each session and will not allow students to access the Internet through their username and password.
- Each child will also have log in details for them to access the school shared area of the network and their own area to store work. These details and access are only available on school grounds and are protected by our network provider.

- **FILTERING INTERNET ACCESS**

- The School uses a filtered Internet service called Securly.
- The School uses E safe Forensic Monitoring to analyse activity on school computers and flag up possible inappropriate use and language.
- The school's Internet provision includes filtering appropriate to the age and maturity of students.
- The school will always be proactive regarding the nature of content, which can be viewed through the School's Internet provision.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and students will be aware of this procedure by reading and signing the ICT Acceptable Usage Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the E-Safeguarding AP. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the E-Safeguarding AP. The school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- The school will regularly review the filtering product for its effectiveness.
- The filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.

- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.

Response to an Incident of Concern



Contact Details

Child Protection Officer for Education: Joanne Dickson 01642 837732

Appendix 1: Acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use Tell my teacher immediately if: ○ I click on a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password Never share my password with anyone, including my friends. • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**