Lingdale Primary School

E-SAFEGUARDING POLICY

Ratified by Governors/Principal:	John Whitehead
Current ratification date:	Spring 2018
Review frequency:	Two years
Next review date:	Spring 2020
Responsibility of:	Sarah Thornton/Sara McCallum

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. 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	1.0
Date	November 2017
Author	Head Safeguarding and E-safety
This e-safeguarding policy was approved by the Governing Body on*:*	
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:	November 2017

Should serious e-safeguarding incidents take place, the following external persons / agencies should be informed:	*Marianne Dixon CPOE Child Protection Officer for Education*

- The school/Academy 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 and at KS4 - KS5 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 Executive Headteacher has overall responsibility for E-Safeguarding all members of the School community, though the day-to-day responsibility for E-Safeguarding will be delegated to the Headteacher for Child Protection and E-Safety.
- 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 Headteacher 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 Use 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.

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 Use Policy with their children.
- 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.

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 Use 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 ICT curriculum.
- We will celebrate and promote E-Safeguarding through a planned programme of assemblies 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 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 Use 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

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.

- **FILTERING INTERNET ACCESS**

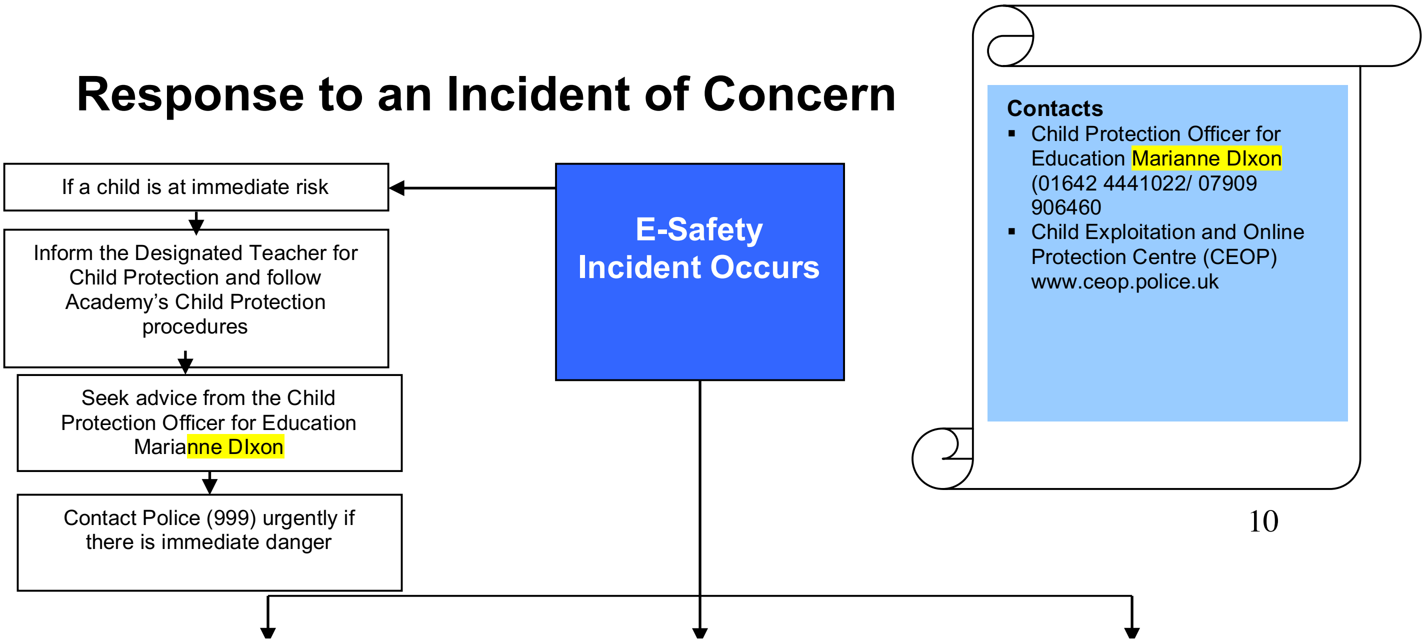
- The School uses a filtered Internet service called Smoothwall.
- The School uses E safe Forensic Monitoring to analyse activity on Academy computers and flag up possible inappropriate use and language.
- The School's Internet provision includes filtering appropriate to the age and maturity of students.
- 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 Use 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.

PASSWORDS

- A secure and robust username and password convention exists for all system access, i.e. email, network access, Academy management information systems etc.
- All staff will have a unique, individually named user account and password for access to ICT equipment and information systems available within the School.
- All information systems require end users to change their password at first log on.
- Users are prompted to change their passwords at pre-arranged intervals, or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise.
- All staff and students have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and students will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.

- All staff and students will sign an ICT Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer-based services, never share these with other users.
    - Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an Internet browser.
- All access to School information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the School's personal data protection policy.
- The School maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + = , < > : : " '): the more randomly they are placed, the more secure they are.

Response to an Incident of Concern



E-Safety Incident Occurs

If a child is at immediate risk

Inform the Designated Teacher for Child Protection and follow Academy's Child Protection procedures

Seek advice from the Child Protection Officer for Education Marianne DIxon

Contact Police (999) urgently if there is immediate danger

Contacts

- Child Protection Officer for Education Marianne DIxon (01642 4441022/ 07909 906460
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk