E-Safeguarding Policy

Redscope Primary School

Title	Redscope eSafeguarding Policy
Version	1.0
Date	05/03/2014
Author	eSafeguarding Co-ordinator
Approved by head teacher	P Dobbin
Approved by governing body	Bronwen Watson
Next review date	05/03/2016

Modification History			
Version	**Date**	**Description**	**Revision Author**

E-Safeguarding Policy

Redscope Primary School

1. Introduction

This policy sets out the key principles expected of all members of the school community at Redscope Primary School with respect to the use of ICT-based technologies to safeguard and protect the children and staff. It aims to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice. It sets clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use. Redscope Primary School must ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken this will therefore minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

2. Scope of policy

This policy applies to the whole school community including Redscope Primary's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils. Redscope Primary's senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this policy. The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other eSafeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will clearly detail its management of incidents within this policy and its anti-bullying policy and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that takes place out of school.

3. Review and ownership

- The school has appointed an eSafeguarding coordinator, Ms.R.Russell, who will be responsible for document ownership, review and updates.
- The eSafeguarding policy has been written by the school eSafeguarding Coordinator and is current and appropriate for its intended audience and purpose.
- The school eSafeguarding policy has been agreed by the senior leadership team and approved by governors.
- The eSafeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The School has appointed a member of the governing body to take lead responsibility for eSafeguarding.

- All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

4. Communication

- Redscope Primary's senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.
- The eSafeguarding policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all members of the school community as and when needed.
- Any amendments will be discussed with the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An eSafeguarding or eSafety module will be included in the PSHE, Citizenship and/or ICT curricula covering and detailing amendments to the eSafeguarding policy within all year groups. The eSafeguarding policy will be introduced to the pupils at the start of each school year and will show progression through the year groups.
- An eSafeguarding or eSafety training programme will be established across the school to include a regular review of the eSafeguarding policy.
- Pertinent points from the school eSafeguarding policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within school.
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used
- The eSafeguarding policy will be introduced to the pupils at the start of each school year and will show progression through the year groups.
- eSafeguarding posters will be prominently displayed around the school.

5. Roles and Responsibilities

Responsibilities of the Senior Leadership Team

The headteacher is ultimately responsible for eSafeguarding provision (including eSafeguarding) for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding coordinator. The headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.

Responsibilities of the E-Safeguarding Coordinator

The role of the E-safeguarding co-ordinator, Ms R Russell, is:

- To promote an awareness and commitment to eSafeguarding throughout the school
- To be the first point of contact in school on all eSafeguarding matters

- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures
- To communicate regularly with school technical staff
- To communicate regularly with the designated eSafeguarding governor
- To communicate regularly with the senior leadership team
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues
- To ensure that eSafeguarding education is embedded across the curriculum
- To ensure that eSafeguarding is promoted to parents and carers
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate
- To monitor and report on eSafeguarding issues to 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 eSafeguarding incident
- To ensure that an eSafeguarding incident log is kept up to date

Regular non-contact time should be provided for the E-safeguarding Coordinator to ensure that her responsibilities can be fulfilled and policies/procedures/incidents can be monitored and reviewed.

Responsibilities of Teachers and Support Staff

All staff within school will be expected:

- To read, understand and help promote the school's eSafeguarding policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any suspected misuse or problem to the eSafeguarding coordinator
- To develop and maintain an awareness of current eSafeguarding issues and guidance
- To model safe and responsible behaviours in their own use of technology
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones or social media, etc.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology
- To ensure that pupils 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 eSafeguarding issues related to the use of mobile phones, cameras and handheld devices
- To understand and be aware of incident-reporting mechanisms that exist within the school
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of Technical Staff

All technical staff will be expected:

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work
- To maintain a professional level of conduct in your personal use of technology at all times
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that access to the school network is only through an authorised, restricted mechanism
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system
- To liaise with the local authority and other appropriate people and organisations on technical issues
- To document all technical procedures and review them for accuracy at appropriate intervals

- To restrict all administrator level accounts appropriately
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

Responsibilities of Pupils

All pupils (through both Key Stages) will be expected:

- To read, understand and adhere to the school pupil Acceptable Use Policy
- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices
- To know and understand school policies on the taking and use of mobile phones
- To know and understand school policies regarding cyber-bullying
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in 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

Responsibilities of Parents and Carers

All pupils and carers will be expected:

- To help and support the school in promoting eSafeguarding
- To read, understand and promote the school pupil 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 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 eSafeguarding 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 agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school
- 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*

    - *Images taken of pupils at school events maybe shared via the internet on the school website. Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.*

    - *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.*

Responsibilities of the Governing Body

The governing body are expected:

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils
- To develop an overview of how the school ICT infrastructure provides safe access to the internet
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school
- To support the work of the eSafeguarding coordinator in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy

Responsibilities of the Child Protection Officer

The designated Child Protection Officer will be expected to:

- 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 Other External Groups

- The school will liaise with local organisations (e.g. CEOP and YHGfL) to establish a common approach to eSafeguarding and the safe use of technologies.

- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate

6. Managing Digital Content

Using images, video and sound

Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published:

On the school website (and in future, a possible blog)
In the school prospectus and other printed promotional material, e.g. newspapers
In display material that may be used around the school
Recorded or transmitted on a video or via webcam in an educational conference

This will be done annually or as part of the home-school agreement on entry to the school. Parents and carers may withdraw permission, in writing, at any time.

We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the headteacher provided that any media is transferred solely to a school device and

deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved.
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.

Storage of Images

Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment. The school may store images of pupils that have left the school for a number of years following their departure for use in school activities and promotional resources. Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils. The ICT advocate has the responsibility of deleting the images when they are no longer required, or when a pupil has left the school.

7. Learning and Teaching

We will provide a series of specific eSafeguarding-related lessons in every year group as part of the ICT curriculum / PSHE curriculum (which will be detailed in the new ICT/Computing Long-Term Plan).We will celebrate and promote eSafeguarding through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.We will discuss, remind or raise relevant eSafeguarding messages with pupils 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.

Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign. Pupils will be taught about the impact of cyber-bullying and know how to seek help if they are affected by any form of online bullying. Pupils 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.

8. Staff Training

Our staff receive regular information and training on eSafeguarding issues in staff meetings and INSET.
As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies. All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community. All staff will be encouraged to incorporate eSafeguarding activities and awareness within their curriculum areas. A log of staff training received in eSafeguarding is kept within school.

9. 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 appropriate. Virus protection is installed on all appropriate hardware, and will be kept active and up to date.

All users will sign an end-user Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked. At Key Stage 1 and Key Stage 2, pupils will access the internet using a user id and password, which the teacher supervises. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times. They will ensure they log out after each session.
Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their id and password. They will abide by the school AUP at all times.

10. Passwords

A secure and robust username and password convention needs to exist for all system access. (email, network access, school management information system).

Key Stage 1 and 2 pupils will have an individual 'pupil' logon and password to all school ICT equipment. All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.

Users should change their passwords whenever there is any indication of possible system or password compromise. All staff 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 pupils will sign an 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.*
>
> *Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures, e.g. emagwriter.*

The school maintains a log of all accesses by users and of their activities while using the system. Passwords should contain a minimum of eight characters and be difficult to guess with numbers, letters and special characters in their passwords. The more randomly they are placed, the more secure they are. Users should create different passwords for different accounts and applications.

11. Emerging Technologies

All new technologies will be tested and reviewed for any security vulnerabilities that may exist. Suitable countermeasures will be adopted within school to ensure that any risks are managed to an acceptable level. Prior to deploying any new technologies within school, staff and pupils will have appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities. Methods to identify, assess and minimise risks will be reviewed regularly.

12. Filtering Internet Access

The school uses a filtered internet service. The filtering system is provided through RGfL using Smoothwall and includes filtering appropriate to the age and maturity of the pupils.

If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Coordinator. All incidents will be documented in the eSafeguarding log.If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such incidents to the filtering provider, RGfL.

Pupils will be taught to assess content as their internet usage skills develop. Pupils will use age-appropriate tools to research internet content. The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

13. Internet Access Authorisations

All staff and pupils will have the appropriate awareness training and sign the pupil Acceptable Use Policy regarding internet access within school. Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability. When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on prior knowledge. Key Stage 1 pupils' internet access will be directly supervised by a responsible adult. Key Stage 2 pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

14. Email

Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked. Pupils will be allocated a class email account for their own use in school. RGfL can make individual email accounts available if required. Pupils may only use school-provided email accounts for school purposes. Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.

Staff will only use official school-provided email accounts to communicate with pupils and parents and carers. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

Email usage

Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes. Pupils and staff will be reminded when using email about the need to send polite and responsible messages. Pupils must not reveal personal details of themselves or others in email communications. Communication between staff and pupils or members of the wider school community should be professional and related to school matters only. Staff email accounts should be checked regularly for new correspondence.

Pupils and staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments. Pupils and staff should never open attachments from an untrusted source. Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately. Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.

15. Using blogs, wikis, podcasts, social networking and other ways for pupils to publish content online

Blogging, podcasting and other publishing of online content by pupils will take place within school and may be published on the school's website. Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.

Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname. Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes.

Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

16. Mobile Phone Usage in School

Staff Use of Personal Devices

Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices. The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones. Personal mobile phones will only be used during lessons with prior permission from the headteacher in exceptional circumstances. No images or videos should be taken on mobile phones or personally-owned mobile devices.

Pupils' Use of Personal Devices

Pupils are advised not to bring his or her mobile phone or personally-owned device into school. Any device brought into school needs to be stored securely by the class teacher. The school accepts no responsibility for the loss, theft or damage of pupils' mobile phones or mobile devices.

Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences. If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will then be released to parents or carers.

If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

17. Data Protection and Information Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.

Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information. All access to information systems should be controlled via a suitably complex password.

Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school. All physical information will be stored in controlled access areas.

All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.

All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted laptops or encrypted hard-drives. Devices taken off site, e.g. laptops, tablets, etc, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

18. Management of Assets

Details of all school-owned hardware will be recorded in a hardware inventory. Details of all school-owned software will be recorded in a software inventory.

All redundant ICT equipment will be disposed of through an authorised agency and ICT equipment that may have held personal data will have the storage media irretrievably destroyed.

Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.