Redlands Primary & Nursery School

e-Safety and Data Security Policy

Members of staff responsible: Head Teacher
Date policy written:
Date approved by the full governing body: November 2018
Date to be reviewed: November 2020

Content

Introduction / Rationale

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning at Redlands in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning.

Over the past 3 years we have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, we must, through our e-safety policy, ensure that we meet the statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

This policy is for the attention of all staff, governors, visitors and pupils associated with Redlands Primary School. It is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, tablets, webcams, whiteboards, digital video equipment, etc); and technologies Computing covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites

E-mail, Instant Messaging and chat rooms

Social Media, including Facebook and Twitter

Mobile/ Smart phones with text, video and/ or web functionality

Gaming, especially online

Blogs and Wikis

Podcasting

Video Broadcasting

Music Downloading

At Redlands, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. As each year group has a blog page, the blogging rules are displayed clearly on home page and children have been instructed to adhere to them, both in school and at home. All posts from children will be reviewed by their class teacher before being posted online, to avoid inappropriate behaviour. Whilst exciting and beneficial both in and out of the context of school, much ICT, particularly web-based resources, are not consistently monitored. Therefore, children are frequently reminded of the range of risks associated with the use of other Internet technologies and that some have minimum age requirements, usually 16 years (Facebook).

The use of new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers

- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Our school holds personal data on learners, staff and other people. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of our school. Everybody at Redlands has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Due to the ever changing nature of Information and Communication Technologies, it is best practice that we reviews the E-Safety/Acceptable Use Policy at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Governing Body on:	
The implementation of this e-safety policy will be monitored by the:	ICT coordinator (P. White) Senior Leadership Team Head teacher (S.Walker)
Monitoring will take place at regular intervals:	Termly: • Work scrutiny • Blog monitoring • Internal monitoring data for network activity. • Surveys / questionnaires of 1. students / pupils (Ofsted "Tell-us" survey & CEOP ThinkUknow survey) 2. parents / carers 3. staff
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-Safety 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:	Annually
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Mr. S Walker (Head Teacher) LA ICT Manager, LA Safeguarding Officer, Police Commissioner's Office

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor (it is suggested that schools consider this being a separate appointment to the Computing Link Governor). The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator.
- regular monitoring of e-safety incident logs.
- regular monitoring of filtering /change control logs.
- reporting to relevant Governors committee /meeting.

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Head teacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher /Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator:
S.Walker G.Willford and L.Hollinger are the named e-safety coordinator for Redlands Primary School.

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- reports regularly to Senior Leadership Team/Governors

Network Manager / Technical staff:
Computing Support Technician / Computing Co-ordinator is responsible for ensuring:

- that the school's Computing infrastructure is secure and is not open to misuse or malicious attack

- that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / blog / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:
are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- digital communications with students / pupils (email /blog / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor computing activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection / Child Protection Officer:
should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school computing systems in accordance with the Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (NB at KS1 it will be that parents / carers who sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of Computing technologies than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, letters, website and the Redlands School blog. Parents and carers will be responsible for:

- endorsing (by signature) the Acceptable Use Policy
- accessing the school website / blog in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school computing systems / website / blog as part of the Extended School provision will be signed in as a 'Community' user with minimum rights to programs/printers/files. Internet filters are on maximum for Community visitors.

eSafety/Acceptable Use Education

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils 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. (Planning and activities for e-safety lessons can be found on Resources drive in 'Esafety Lessons' folder.)

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

- A planned e-safety programme should be provided as part of Computing/ PHSE and should be revisited annually– this will cover both the use of Computing and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Students / pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of Computing equipment, the internet and mobile devices both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on laptop trollies.
- Staff should act as good role models in their use of technology, the internet and mobile devices.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, blog
- Reference to eSafety websites through life channel

Education & Training – Staff

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. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety coordinator will receive regular updates through eSafety newsletters/ emails/ training sessions and by reviewing guidance documents released by BECTA / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety coordinator will provide advice / guidance / training as required to individuals as required

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities

- School Computing systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school Computing systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- When accessing the school blog, users will be made responsible for the security of their username and password. They must not allow other users to access the blog using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- In the event of the Computing coordinator needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher
- Any filtering issues should be reported immediately to EMBC.
- Requests from staff for sites to be removed from the filtered list will be considered by the Computing coordinator and EMBC
- School technical staff regularly monitor and record the activity of users on the school Computing systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (eSafety report sheet to be completed by class teacher on behalf of child).
- The school infrastructure and individual workstations are protected by up to date virus software Appropriate anti-virus/security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- We do not allow staff to install programmes on school workstations / portable devices. This has to be discussed and agreed by the Computing coordinator and installed correctly by the Computing technician.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of Computing technology across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the service provider can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be discussed with the head teacher, with clear reasons for the need.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils 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 / pupils 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 eg 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.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and blog.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies eg few schools allow pupils to use mobile phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the pupils. A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks /disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	√						√	
Use of mobile phones in lessons (if mobile phone is used for personal blogging device)		√						√
Use of mobile phones in social time	√							√
Taking photos on mobile phones or other camera devices (for blogging and immediate deleting afterwards)		√						√
Use of hand held devices eg PDAs, PSPs		√						√
Use of personal email addresses in school, or on school network		√						√
Use of school email for personal emails				√				√
Use of chat rooms / facilities				√				√

Use of instant messaging				√				√
Use of social networking sites				√				√
Use of blogs	√				√			

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the e-safety coordinator – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents / carers (email, blog etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other computing systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Redlands believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	Unaccepta	Unaccepta ble and
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X

	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					X	

Responding to incidents of misuse

Pupils	Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of	Refer to Headteacher	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).						X	X		
Unauthorised use of non-educational sites during lessons	X					X			
Unauthorised use of mobile phone / digital camera / other handheld device	X					X			
Unauthorised use of social networking / instant messaging / personal email	X				X	X			
Unauthorised downloading or uploading of files		X			X	X	X		
Allowing others to access school network by sharing username and passwords		X			X	X	X		
Attempting to access or accessing the school network, using another student's / pupil's account			X		X	X	X		
Attempting to access or accessing the school network, using the account of a member of staff			X		X	X	X		
Corrupting or destroying the data of other users			X			X	X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			X			X	X		
Continued infringements of the above, following previous warnings or sanctions			X			X	X	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X		X	X	X	X	
Using proxy sites or other means to subvert the school's filtering system			X		X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X			

Deliberately accessing or trying to access offensive or pornographic material			X		X	X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X	X	X	X		

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).								
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data eg holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature								
Using personal email / social networking / instant messaging / text								

messaging to carrying out digital communications with students / pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school								
Using proxy sites or other means to subvert the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Appendices

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Report to the Headteacher and e-Safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Headteacher immediately.

Ensure the device is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:
Preserve any evidence.
Inform the Headteacher immediately and follow Child Protection Policy as necessary.
Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the e-Safety Leader if this is deemed necessary.

Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform LA/RBC as above.

C. A child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Headteacher and Designated Person for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence.
Inform the Headteacher immediately.
Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

Redlands Primary & Nursery School

Redlands Primary School E-Safety Incident Log

Details of **ALL** eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT and Governors.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (include print out of evidence to be kept in the folder)	Actions and reasons

Redlands Primary & Nursery School

Redlands School Acceptable Use Agreement / e-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT and Fronter username and passwords.
- ✓ I will only open my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Name:_____ Signed _____ Date_____

Redlands Primary & Nursery School

Redlands Primary School

These are our rules for using the Internet safely.

Our Internet Rules

- ✓ We use the Internet safely to help us learn.
- ✓ We learn how to use the Internet.
- ✓ We can send and open messages with an adult.
- ✓ We can write polite and friendly e-mails or messages to people that we know.
- ✓ We only tell people our first name.
- ✓ We learn to keep our usernames and passwords a secret.
- ✓ We know who to ask for help.
- ✓ If we see something we do not like we know what to do.
- ✓ We know that it is important to follow the rules.
- ✓ We are able to look after each other by using our safe Internet.
- ✓ We can go to www.thinkuknow.co.uk for help.

Useful websites

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk – (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)
- www.becta.org.uk (advice for settings to update policies) and http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)
- www.nen.org.uk (for schools and settings – access to the National Education Network)