Policy Documentation

E-safety

OUR VISION

To ensure the safeguards and awareness of all employees and pupils; enabling them to make informed and safe decisions

Relationship to other Policies	**Date**	**Status**
• Child Protection • Bullying • Curriculum • Data Protection • Security • Mobile phone	February 2016	Governor Approval
	February 2017	Review

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these 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 games / film / content
- 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 including (but not limited to) those listed on the front of this policy document.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build 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. All schools must demonstrate that they have provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

The e-safety policy that follows explains how Reevy Hill Primary School intends to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

This e-safety policy has been developed by:

- Headteacher and Senior Leaders
- Teachers
- ICT Technical staff
- Governors

Consultation with the whole school community has taken place through the following:

- Staff meetings and training
- Whole school assemblies and specialist workshops within years 4-6

The implementation of this e-safety policy will be monitored by the governors and the

Headteacher and/or SLT. 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 February 2017. Should serious e-safety incidents take place the Lead Officer for Child Protection for Bradford will be informed.

The school will monitor the impact of the policy using:
- Logs of reported incidents (via e-safe)
- Internal monitoring data for network activity (via e-safe)
- Regular discussions with pupils.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and/or equipment, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy (and associated Behaviour and Anti-bullying policies) and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. Governors will receive regular information about e-safety incidents and monitoring reports (using e-safe)

Headteacher and Senior Leaders are responsible for ensuring the safety (including e-safety) of members of the school community. They:
- Ensure relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Receive and process regular monitoring reports.
- Follow procedures in the event of a serious e-safety allegation being made against a member of staff. (Refer to the Managing Investigations Against Staff Policy.)

E-safety lead 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. They:
- Provide training and advice for staff
- Liaise with the Local Authority
- Liaise with school ICT technical staff
- Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Technical staff ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack. They ensure that:

- The school meets agreed e-safety technical requirements.
- Users may only access the school's networks through a properly enforced password protection policy (To be in place by May 2016)
- They keep 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.

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 ensure:

- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Headteacher for investigation, action and/or sanction
- All digital communications with pupils and parents (email/blogs/voice) are on a professional level and are only carried out using official and/or approved 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 are taught about cyber-bullying, the risks and dangers of this and how to seek help if this is happening to them. Additionally, staff will make it clear to pupils that any incidents of cyber-bullying will be dealt with in accordance with the school behaviour policy and that this will also cover their actions out of school, if any incidents occur that are related to their membership of the school.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They actively monitor ICT 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 are 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

Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy. They know and understand:

- To avoid plagiarism and uphold copyright regulations when carrying out research.
- The importance of reporting of abuse, misuse or access to inappropriate materials and how to do this.
- School policies on the use of mobile devices. They also know and understand school policies on the taking/use of images and on cyber-bullying.
- 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 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 ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/and information about national/ ocal e-safety campaigns. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Ensuring they and their children follow this when using digital technologies at home, related to their membership of the school

Community Users who access school ICT systems/website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems. This will be tailored to the specific needs of the group.

Technical – infrastructure/equipment, filtering and monitoring and the role of the Network Manager

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical standards as required by City of Bradford Metropolitan District Council.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by our ICT technical support service who will keep an up to date record of users and their usernames. (To be in place by May 2016)
- The administrator passwords for the school ICT system, used by Technical Staff (or other person) must also be available to the Headteacher (or other nominated senior leader) and kept in a secure place (eg school safe). Only the headteacher (or other nominated person) can grant permission to access any school system as an 'administrator'.
- Users will be made responsible for the security of their username and password, 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.
- The school has provided enhanced user-level filtering through the use of the e-safe system and the Smoothwall installation
- Any filtering issues should be reported immediately to BLN
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. (By May 2016)
- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices without permission from the e-safety lead or headteacher.
- An agreed policy is in place regarding the use of removable media (by users on school workstations / portable devices)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data is not sent over the internet to 'external' email addresses or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

Reevy Hill subscribes to The Innovation Centre Bradford's online curriculum service to ensure staff have access to high quality, up to date and relevant resources. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum, using The Innovation Centre Bradford's online resources to assist with this. Through the use of these curriculum resources pupil e-Safety will be provided in the following ways:

- A planned e-safety programme will be provided as part of the curriculum and will be regularly revisited. This will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils will 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
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff will act as good role models in their use of ICT, the internet and mobile devices.

All staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be as follows:

- A planned programme of formal e-safety training for staff.

- New staff will 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 lead will receive regular updates through attendance at appropriate network events and briefing sessions.
- Frequent discussions about this policy and implementation will take place throughout the year during briefing sessions, staff meetings and INSET training days.

Carrying out internet searches

Where 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. Primary Safe Search should be the default search engine used by pupils however we also recognise that it is essential that older pupils, particularly those in Phase 3, are taught how to safely search using more mainstream search engines such as Google or Bing.

If pupils are allowed to use these search engines as part of a specific activity staff will:

- Be mindful of the fact that, despite a high level of filtering in place in school, pages and images that are unsuitable for pupils may still arise whilst searching.
- Compose a list of specific words that pupils are allowed to use and then, as part of lesson preparation, search for these terms to minimise the possibility that pupils will find pages or images that may be unsuitable for them. If necessary, staff will change the term that is searched for or use a different search engine.
- Ensure that pupils are given specific limits about how many pages of webpages or images pupils may explore (e.g. if the staff member has checked the first page of image thumbnails only, pupils may only use this page whilst searching.)
- Demonstrate extra vigilance during the lesson.
- Ensure pupils are clear about what they should do if they find an image or webpage upsetting or disturbing or unsuitable.
- Ensure that pupils are reminded of their obligations under the pupil AUP and the consequences of not following this agreement.

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs and discrimination) or use online resources (e.g. educational games) that would normally result in internet searches being blocked. In such a situation, staff can request that those sites are removed from the filtered list for the period of study. Any request to do so, should be sent via email to the headteacher, including a link and a clear reason for the need.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate 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, however images must only be taken on school equipment. The personal equipment of staff must not be used for such purposes. Staff 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 students/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, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

- All digital and video images will be stored securely on school owned equipment or networks until they are no longer needed. Images or videos must not be stored on personal equipment. Images and video will be deleted at the earliest opportunity, once their use has passed. Staff and pupils will ensure digital images and videos are deleted from 'shared' equipment (e.g. iPads, cameras etc) before returning these to central storage.

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.

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 and store personal data only on secure password protected computers and devices belonging to the school (By May 2016)
- Are properly "logged-off" at the end of any session in which they are using personal data.

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
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, once it has been transferred or its use is complete

Communications (including email, the use of social networks and mobile phones)

When using communication technologies the school considers the following as good practice:

- The official school email service (name@reevyhill.bradford.sch.uk) may be regarded as safe and secure and is monitored. Likewise the official CBMDC email service (name@bradford.gov.uk) may also be considered in the same way. Regardless of this, all staff still need to be cautious about communicating identifiable personal information using these systems and avoid this whenever possible. If in doubt, staff should still check with the e-safety lead or headteacher before sending identifiable personal information via email to these addresses.
- Sending identifiable personal information via email to ANY other email address MUST be agreed by the headteacher or e safety leader first. Emails containing identifiable personal data which need to be sent to external email accounts will be sent through EgressSwitch.
- Staff must ensure they do not leave their email account logged in and unattended at any time.
- Staff and pupils may only use official email accounts on the school system and equipment.
- Users need to be aware that email communications may be monitored
- Users must immediately report to the headteacher or e-safety lead 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 must be professional in tone and content.
- Emails sent to external organisations must be composed, written and treated with the same care as letters written on school headed paper.

- 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.
- Staff are not permitted to use school equipment to access social networking sites at any time. Any access made using personal, privately owned equipment is entirely at the staff member's discretion and risk with no responsibility falling to Reevy Hill Primary School for any consequences of any such access. Any such access must only ever be made from the staff room and NOT from any public areas of the building.
- Staff must not "friend" or communicate with parents or pupils on social networking sites. This advice is given to protect both the individual's and the school's reputation and in the interests of child protection (safeguarding) issues.
- Staff must act to maintain a positive reputation of the school at all times when using social networking sites, even if this is in their own time and on their own equipment.
- Mobile phones will not be used for personal use during formal school time and should be switched off and out of sight at all times when in the presence of pupils.
- When on a school trip staff may use their personal phones to contact school and should NOT contact parents directly.

Assessing risks.

Reevy Hill Primary School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor CBMDC can accept liability for the material accessed, nor any consequences of the internet access. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The school audits ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

Complaints.

Any complaints of internet misuse will be handled using procedures listed in the School Complaints procedure. Complaints of a safeguarding nature will be dealt with in accordance with school safeguarding procedures.

Policy written: Feb 2016
Approved on:
Planned review date: Feb 2017