Billesley Primary School

Draft E- Safety Policy

Executive Principal: Johanne Clifton
Chair of Governors: Chris Blythe
ICT Manager: Jonathan Stamp
September 2016

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- 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 social and emotional development and learning
- Inappropriate use of social media

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and leadership

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.
It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT

Responsibilities: ICT Leader

Our ICT Leader is the person responsible to the Principal and governors for the day to day issues relating to e-safety. The e-safety Leader:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- meets with e-safety governor to discuss current issues, review incident logs and filtering change control logs
- attends relevant meetings and committees of Governing Body
- reports regularly to the Principal
- Ensures the ICT Manager
  - liaises with The Elliott Foundation (TEF)
  - receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
  - reports regularly to the Principal
  - receives appropriate training and support to fulfil their role effectively
  - has responsibility for blocking / unblocking internet sites in the school's filtering system / passing on requests for blocking / un blocking to the ICT Helpdesk
  - maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

Responsibilities: Governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. 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 which involves:

- regular meetings with the ICT Leader with an agenda based on:
  - monitoring of e-safety incident logs
  - monitoring of filtering change control logs
  - monitoring logs of any occasions where the school has used its powers of search and deletion of electronic devices
  - reporting to relevant Governor's' committee/meeting

Responsibilities: Principal

- The Principal is responsible for ensuring the safety (including e-safety) of members of the school community, although the day to day responsibility for e-safety is delegated to the ICT Leader.

- The Principal and Vice Principal will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Responsibilities: classroom based staff

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's Acceptable Use Policy for staff
- they report any suspected misuse or problem to the ICT Leader or ICT Manager
- digital communications with students (email / voice) will be on a professional level and only carried out using official school systems
- e-safety issues are embedded in the curriculum and other school activities.

Responsibilities: ICT Manager

The ICT Manager is responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the Principal or Vice Principal so that appropriate action may be taken.

Policy development, monitoring and review

This e-safety policy has been developed by a working group made up of:

- ICT Leader
- ICT Manager
- Principal and Vice Principal
- Governors (especially the e-safety governor)
- Pupils

Schedule for development / monitoring / review of this policy

The implementation of this e-safety policy will be monitored by the:	The health and safety committee under the direction of the ICT Leader
Monitoring will take place at regular intervals:	Annually
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:	September 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	The Elliott Foundation (TEF)

Policy Scope

This policy applies to all members of the school community (including but not limited to staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Principals, 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.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign their consent before being given access to school systems.

Acceptable use policies are provided for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)

- Parents / carers when accessing the school system

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

When a child enters the school, parents are informed that children will be using the school's internet resources and that their child's image (still or moving) and their child's work may be published within school and/or on the school website, school blog or the school's twitter feed. If a parents/carers do not wish their child's image to be used then this preference is recorded on school records. A list of pupils whose image should not be published is produced and updated by Senior School Secretary. This list is made available to all staff.

Induction policies for all members of the school community include this guidance.

Self-Evaluation

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parents, teachers and governors) are taken into account as a part of this process.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT Policies

ICT Policy: How ICT is used, managed, resourced and supported in our school
E-Safety Policy: How we strive to ensure that all individuals in school stay safe while using ICT. The e-safety policy constitutes a part of the ICT policy.

Other policies relating to safety

Anti-bullying: How our school strives to illuminate bullying – link to cyber bullying
PSHE: E-Safety has links to this – staying safe
Safeguarding: Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy
Behaviour: Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context: **some are illegal**. Users will not engage in these activities when using school equipment or systems (in or out of school). 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 (illegal - The Protection of Children Act 1978)
- grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- 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

Additionally the following activities are considered unacceptable on ICT kit provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Birmingham Local Authority and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- 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
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupil Sanctions	Refer to class teacher	Refer to e-safety coordinator	Refer to Principal or Vice Principal	Refer to Police	Inform parents/ carers	Removal of network/ internet access	Warning	Further sanction e.g. detention/ exclusion
Deliberate accessing or trying to access material that could be considered illegal (see previous list)	√	√	√		√	√	√	√
Unauthorised use of non-educational sites during lessons	√				√	√		
Unauthorised use of mobile phone/ digital camera/ other handheld device	√		√		√			
Unauthorised use of social networking/ instant messaging/ personal email	√		√		√			
Unauthorised downloading or uploading of files	√						√	
Allowing others to access the school network, using the account of a member of staff	√	√	√		√	√	√	
Attempting to access or accessing the school network, using another pupil's account	√	√	√			√	√	
Attempting to access or accessing the school network, using the account of a member or staff	√	√	√		√	√	√	
Corrupting or destroying the data of other users	√	√	√		√	√	√	
Sending an email, text, or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√		√	√	√	√
Continued infringements of the above, following previous warnings or sanctions	√	√	√	√	√	√	√	√
Actions which could bring the school into disrepute or breath 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 flailing to report the incident	√	√	√		√			
Deliberately accessing or trying to access offensive or pornographic material	√	√	√	√	√	√	√	√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	√	√	√		√	√	√	

Staff Sanctions	Refer to line manager	Refer to Principal or Vice Principal	Refer to Tefat	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberate accessing or trying to access material that could be considered illegal (see previous list)	√	√	√	√	√	√	√	√
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/ accessing the school network, using another person's account	√	√				√		
Careless use of personal data e.g 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 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 carry out digital communications with 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 flailing 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	√	√	√			√	√	√

Audit / Monitoring / Reporting / Review

The ICT Manager will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Principal or Vice Principal and a governor on a termly basis.

Use of handheld technology (USB, personal phones and handheld devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- The use of USB sticks are not permitted in school unless approved by SLT and encrypted.
- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
    - Personal handheld devices will be used in lesson time only in an emergency or extreme circumstances
    - Members of staff are free to use these devices in school, outside teaching time.

Email

Access to email is provided for all users in school via the intranet page accessible via the web browser from their desktop.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils will use only the school email services to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Pupils have access to an individual email account for communication within school.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Staff may only access personal email accounts on school systems outside of teaching hours.
- Users must immediately report, to their class teacher / e-safety coordinator – in accordance with the Safeguarding 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.

Use of digital and video images

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images will only be captured using school equipment; the personal equipment of staff will not be used for such purposes.
- Care will 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.

Use of web-based publication tools

Our school uses the public facing website, http://www.billesleyschool.co.uk/ and the school's blog, facebook page and twitter feed for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) will be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - Pupils' full names will not be used anywhere on a website, blog, facebook or twitter and never in association with photographs
    - Photographs of pupils will not be published where parents/carers have requested that the school do not publish images of their child(ren).

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE https://www.gov.uk/government/publications/teachers-standards Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, VLE 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 technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from RM Education we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the ICT Manager (with ultimate responsibility resting with the Principal or Vice Principal and governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

All users have a responsibility to report immediately to class teachers, ICT Leader, ICT Manager or another adult in school any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe will be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- briefing in staff meetings, training days, and further updates as necessary.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Audit / reporting

Logs of filtering change controls and of filtering incidents are made available to

- the e-safety governor
- The Elliott Foundation (TEF)

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

E-safety education

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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

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

- A planned e-safety programme will be provided as part of ICT, PHSE and other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hector's World at KS1 and Cyber Café at KS2)

- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.

- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.

- In lessons where internet use is pre-planned, it is best practice that pupils will 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 pupils are allowed to freely search the internet, e.g. using search engines, staff will be vigilant in monitoring the content of the websites the young people visit.

Information Literacy

- Pupils will be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:
    - o Checking the likely validity of the URL (web address)
    - o Cross checking references (can they find the same information on other sites)
    - o Checking the pedigree of the compilers / owners of the website

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Pupils are taught how to make best use of internet search engines to arrive at the information they require

The contribution of the children to e-learning strategy

It is our school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy.

Staff training

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The ICT Leader and ICT Manager will receive regular updates through attendance at TEF or other information / training sessions and by reviewing guidance documents released by the DfE.
- The ICT Leader will provide advice, guidance and training as required to individuals as required on an ongoing basis.

Governor training

Governors take part in e-safety training and awareness sessions. This is offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or Learning and Achievement Service), National Governors Association and TEF.
- Participation in school training / information sessions for staff or parents

The e-safety governor works closely with ICT Leader and reports back to the full governing body.

Parent and carer awareness raising

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 and regulation of the children's online 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
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) and other

sites where appropriate.

Wider school community understanding

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety will also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

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.