

Beaconsfield Primary School



E-Safety Policy

January 2011

Date approved by governors: March 2011
Review date: January 2013

E-safety Policy

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology 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
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Beaconsfield Primary, we understand the responsibility to educate our pupils on eSafety 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. Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in our school is Helen Towers who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Ealing LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ eSafety co-ordinator and governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's ICT policy and acceptable use agreements for staff, governors, visitors

and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, behaviour/pupil discipline (including the anti-bullying) policy and PHSE.

eSafety skills development for staff

- The eSafety co-ordinator has attended accredited training on issues relating to eSafety and cyber bullying in November 2010.
- A staff meeting was conducted in January 2011 to inform staff of the key information about eSafety and cyber bullying. This training included: information about the risks associated with ICT; an explanation of the different technologies involved (including those such as social networking and gaming sites which our children are likely to be accessing at home); strategies to teach the children to help them stay safe (the SMART rules and the STOP, BLOCK, SAVE, TELL rules relating to cyber bullying). All the resources relating to this staff meeting have been made available on the shared drive for staff to access when necessary. Further training will be ongoing.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas. In the second half of Spring Term 2011 PSHE lessons will be exclusively devoted to eSafety and Cyber bullying activities.
- New staff receive information on the school's acceptable use policy as part of their induction.

Managing the school eSafety messages

- The school has adopted the SMART rules as a consistent approach through the school to teach children about issues relating to eSafety. Posters explaining the SMART rules are displayed in every classroom (see Appendix) and teachers are encouraged to refer to these during lessons involving the use of ICT.
- The SMART rules have been introduced to children by the eSafety co-ordinator through a whole school assembly which was followed up with work in individual classes.
- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.
- In the second half of Spring Term 2011 PSHE lessons will be exclusively devoted to eSafety and Cyber bullying activities. eSafety issues will then continue to be addressed through the PSHE curriculum.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school provides opportunities within a range of curriculum areas to teach about eSafety. In the second half of Spring Term 2011 PSHE lessons will be exclusively devoted to eSafety and Cyber bullying activities. eSafety will then be addressed through the PSHE curriculum and through activities across the curriculum areas whenever ICT is being used.
- In order to support staff in delivering effective lessons on eSafety and cyber bullying which build on previous learning, age appropriate resources have been assigned to each year group. These resources include videos, activities, lesson plans, songs etc. and have been placed on the shared drive for all teachers to access as and when needed. They are as follows:
- Year 1 - Lee and Kim

- Year 2 - Hector's World
 - Year 3 - Dongle the Rabbit
 - Year 4 - Smart Crew
 - Year 5 - Cyber Cafe
 - Year 6 - Cyber bullying/Us Online
- The school promotes the following rules in relation to Cyber Bullying: STOP, BLOCK, SAVE and TELL. This encourages pupils not to reply to or react to cyber bullying, to block bullies from accessing them whenever possible (e.g. by blocking the email address etc.), to save any evidence of bullying and to tell a trusted adult if they become the victim of cyber bullying.
 - Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
 - Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
 - Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
 - Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Users are provided with an individual network, email and Learning Platform log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If they think their password may have been compromised or someone else has become aware of their password report this to the eSafety co-ordinator or Head teacher.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and the MLE including ensuring that passwords are not shared. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the MLE to the browser/cache options (shared or private computer).
- In our school, all ICT password policies are the responsibility of the ICT co-ordinator and all staff and pupils are expected to comply with the policies at all times.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the London Grid for Learning (LGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Ealing Local Authority has a monitoring solution via the London Grid for Learning. Upon request, web-based activity can be monitored and recorded.
- School internet access is controlled through the LGfL's web filtering service.
- Beaconsfield Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off and the incident reported immediately to the e-safety co-ordinator. The offending URL will reported to the LA / LGfL.
- Sophos Anti-Virus protection is provided by the LGfL and is set to automatically update on all school machines. This is the responsibility of the ICT technician.
- In addition staff laptops used at home can also be protected by Sophos Anti-Virus as agreed by the LGfL.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head teacher or ICT co-ordinator.
- If there are any issues related to viruses or anti-virus software, the ICT technician should be informed via the ICT issues log book (kept in the Head teacher's office).

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school.
- Pupils are introduced to Web2 tools within the safe context of the London MLE
- Staff understand that it is highly inappropriate to use open social networking sites (Facebook, MySpace, Bebo etc), and public chat room facilities with pupils. They are expected to use the tools within the MLE.

Mobile technologies

Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones):

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Pupils are not allowed to bring personal mobile devices/phones to school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Capturing images and video is **not** allowed by students or staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school. Staff are responsible for ensuring that school laptops are only used for school purposes and that there is no inappropriate or illegal content on the device.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own LGfL StaffMail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts (MLE Stickies / MLE "Visual Mail") on the school system and only under direct teacher supervision for educational purposes.
- LGfL StaffMail is subject to mail scanning.
- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive message and keep the offending message(s) as evidence.
- Staff must inform the eSafety co-ordinator or Head teacher if they receive an offensive e-mail.
- Pupils are introduced to email as part of the curriculum where appropriate.

Safe Use of Images / Film

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore are easy to misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are **not permitted** to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.
- Images of pupils are deleted when pupils leave the school.

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's MLE
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time.

- Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.
- Video is only streamed from the LGfL VideoCentral service set to private.

Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network and MLE.
- Class teachers have the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are the Head teacher and admin staff. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of instances of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- Participants in conferences offered by 3rd party organisations must be CRB checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Misuse and Infringements

Complaints

Complaints relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged (see Incident Log in Appendix) and process should be followed (see Flowchart in Appendix).

Inappropriate material (staff)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials on school equipment both within and outside school by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct through access to the eSafety policy when signing the acceptable use agreement.

Inappropriate material (pupils)

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials on school equipment will result in sanctions according to the behaviour policy. The child involved may be prevented from accessing ICT within school for a fixed

period. They may also be prevented from accessing the MLE if appropriate. The sanctions given will be at the discretion of the Head teacher.

- Pupils are made aware of the sanctions when signing the acceptable use agreement.

Child Protection

- Any concerns that staff have relating to child protection **must** be reported immediately to the Head teacher or the Assistant head as per Child Protection procedures.

Parental Involvement

We believe that it is essential for parents and carers to be fully involved with promoting eSafety both in and outside of school. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign home school agreements which relate to appropriate use of ICT on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in the form of; Posters, Website/ Learning Platform postings and Newsletter items.
- Parent council has been informed of the school's approach to eSafety issues and letters have been sent home informing parents of the SMART rules being taught throughout the curriculum. During Spring term 2011 the eSafety co-ordinator will be running a workshop for parents on issues relating to eSafety and cyber bullying.

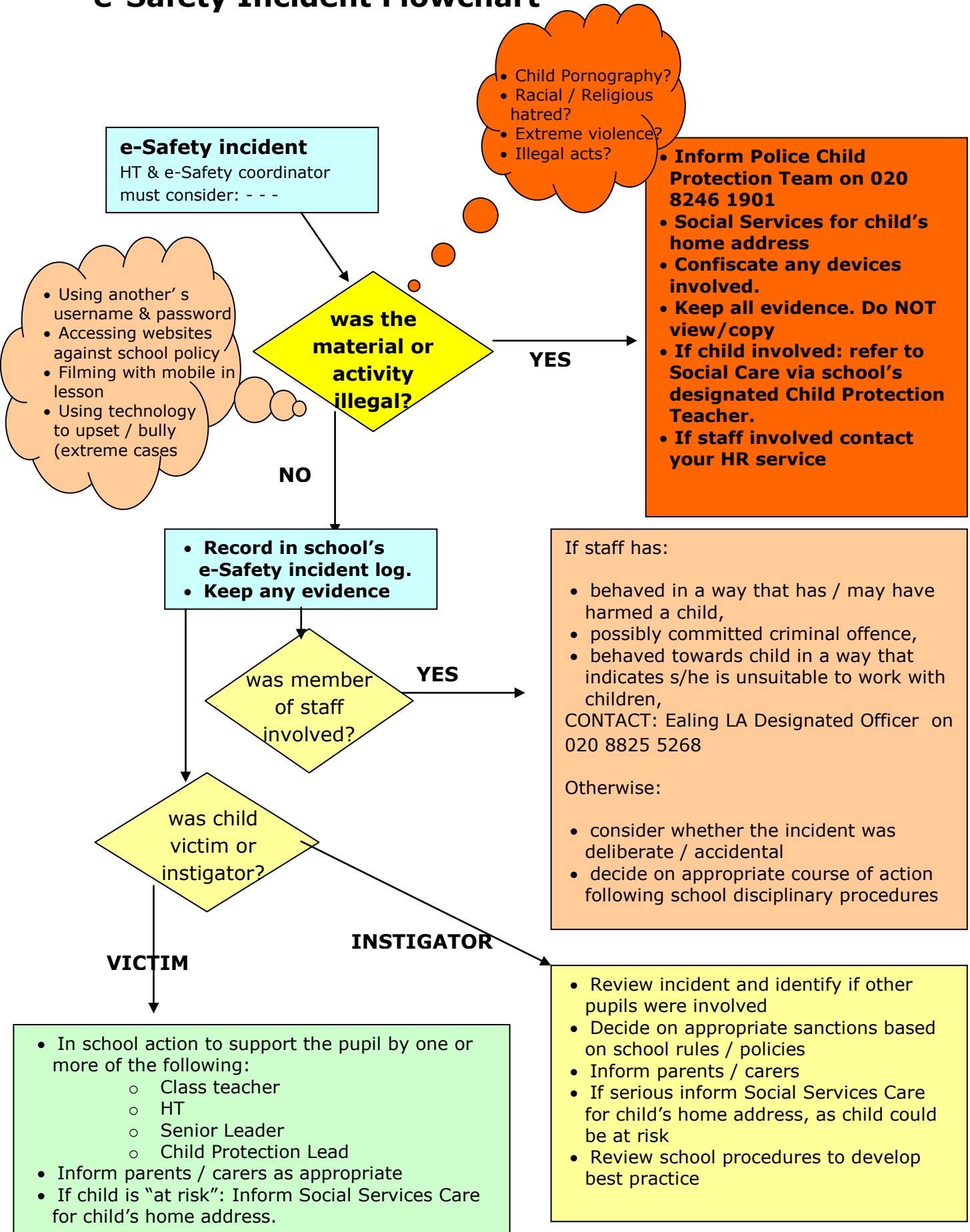
Review Procedure

- There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.
- This policy will be reviewed every 2 years and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Appendix

1. eSafety incident Flow chart
2. Acceptable Use Agreement for Staff
3. Acceptable Use Agreement for Pupils
4. Incident Log
5. SMART rules information sheet displayed in classrooms
6. Information about current legislation relating to eSafety

e-Safety Incident Flowchart



Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Helen Towers, school eSafety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform / MLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role, and never via personal email / phone.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) and MLE tools for communications with pupils / students / parents.
- I am aware that communicating with students / pupils via private email / SMS and social networking sites may be considered a disciplinary matter in this school.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Head Teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- **Understand that to do so may constitute a disciplinary offence and in some cases a criminal offence.**
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature..... Date

Full Name(printed)

Job title

Primary Pupil Acceptable Use

Agreement / eSafety 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 passwords OR use any one else's.
- ✓ I will only open/delete 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.
- ✓ I will not give private details (home address, mobile number, email address etc) to people I meet online.

Dear Parent/ Carer

ICT including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Miss Towers.

✂

Parent/ carer signature

We have discussed this and(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Beaconsfield Primary School.

Parent/ Carer Signature

Class Date

Beaconsfield Primary eSafety Incident Log

Details of any incidents relating to eSafety to be recorded by the eSafety co-ordinator. This will then be reviewed termly by the Head teacher.

- Child protection issues should be reported immediately to the Child Protection officers (Dave Woods or Sumen Starr)
- Any incidents relating to cyber bullying should follow bullying policy.
- See eSafety policy for guidance about sanctions relating to misuse.

Date and Time	Name of pupil or staff member	Male or Female	Room and computer number	Details of incident (including evidence)	Actions taken and reasons for them

SMART!

Safe

Never give out personal information to people you don't know. This includes your full name, where you live, your mobile or home phone number, the name of your school or your email address. Remember that people may not be who they say they are online.

Meet

Never meet up with someone who you have only have talked to online or on your mobile. They may seem nice but they could be dangerous. If someone online asks to meet up with you tell an adult about it.

Accepting

Be very careful about accepting emails, files, instant messages or texts from people you don't know. They could contain upsetting messages or viruses which could break your computer. It is best to delete them straight away and tell an adult about it.

Reliable

Always check the information you get online is correct. You can do this by checking more than one website, using a book or asking an adult. Also remember that people online might be lying about who they say they are.

Tell

Always tell a trusted adult if you or someone you know sees something or receives a message that upsets or worries you or them. Sending nasty messages online or in texts is bullying and is not acceptable in our school.

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they

are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information

www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 - 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 - 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.