Beaconsfield Primary School

'Shining a Light on Learning'

B – Belief

P – Perseverance

S – Success

E-Safety Policy

January 2016

Review date: January 2018

Beaconsfield Primary School
E Safety Policy

Beaconsfield Primary School takes the safety of all children and adults very seriously. This policy is written to protect all children and adults. We recognise that E-Safety encompasses not only Internet technologies, but also electronic communications such as mobile phones and wireless technology.

What does electronic communication 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.

This e-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety coordinator in our school is **Mrs Philippa Stubbs** 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 E-Safety Coordinator to keep abreast of current

issues and guidance through organisations such as Ealing LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/E-Safety coordinator 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 Computing 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.

E-Safety skills development for staff

- The E-Safety coordinator has attended accredited training on issues relating to E-Safety and cyber bullying.
- A staff meeting takes place each year to inform staff of the key information about E-Safety and cyber bullying. This training includes: 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 these staff meetings are made available on the shared drive for staff to access when necessary.
- E-safety lessons are incorporated into both the PSHE and Computing schemes of work and pupils are reminded of protocol each time they use the internet and/or related technologies.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's acceptable use policy as part of their induction.

E-Safety in the Curriculum

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

- E-safety lessons are currently taught as part of the yearly Computing and PSHE schemes of work.
- In order to support staff in delivering effective lessons on E-Safety 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.
- 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. The CEOP 'report abuse' button has also been embedded on the front page of the school's website and in the E-Safety section.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing 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.
- All children are provided with an individual USO log on and user name. From Year 2 upwards they are expected to log on to school computers and laptops using these details.
- Pupils are not allowed to deliberately access online 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 E-Safety coordinator or Head teacher.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks ensuring that passwords are not shared. Individual staff users must also make sure that workstations are not left unattended and are locked.
- In our school, all ICT password policies are the responsibility of the school's 'Nominated Contacts' 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.

- Children at Beaconsfield will have access to the internet however they must be supervised at all times.
- Staff will preview any recommended sites before use.
- Child-friendly search engines are recommended and 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.

Infrastucture

- 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 Coordinator. 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.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head teacher or Computing coordinator.
- 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).

School Website

- The Head teacher and E-Safety officer takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers: Eg. Administration staff.
- The school website complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g admin@beaconsfield.ealing.sch.uk

Social networking sites

- At present, the school endeavours to deny access to social networking sites to pupils within school.
- If they are using social networking sites at home, pupils are advised to be very cautious about the information they share with others.
- 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.
- Staff understand that it is highly inappropriate to use open social networking sites (Facebook, Twitter & photo sharing sites), and public chat room facilities with pupils and disciplinary action will be taken.

Mobile technologies

Many existing mobile technologies such as portable media players, PDAs, tablets, 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.
- Staff use of personal devices is not permitted within the presence of pupils. Use should only occur during break and lunch periods and only in the staffroom/PPA room.
- 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 or social networking messages between any member of the school community is not allowed. This is a potential disciplinary offence.
- Capturing images and video is **not** allowed by students or staff unless on school equipment and only for educational purposes (See the Photographic and Video Images Policy).
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Managing email/blogging

The use of email and blogs within most schools are an essential means of communication for both staff and pupils. In the context of school, emails and blogs 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 or blog post in relation to their age and good 'netiquette'. In order to achieve the objectives set out in the National Curriculum, pupils must have experienced sending and receiving emails and posting on blogs in order to communicate with each other.

- 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. These email accounts are the only ones accepted for use in school.
- 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.
- 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 communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must only publish blog posts within an appropriately secure environment: the school's learning environment/LGfL secure platforms such as J2Webby/J2Bloggy, etc.

- All blog posts and comments must be moderated by staff before being published.
- 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 E-Safety Coordinator 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

Please see the school's 'Photographic and Digital Images Policy' for more details.

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 and back 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/capturing images/video for multimedia projects that will not be published on the internet.
- 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/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 Head teacher 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.

Data security

The access to and appropriate use of school data is something that the school takes very seriously.

- Personal data (such as data held on SIMS) must be kept secure and used appropriately.
- Staff should not take any personal data out of school in paper form or on a USB stick, unless it is encrypted.
- The school is currently investigating the possibility of introducing remote access to remove the need for any information to be transported on USB sticks. If this takes place then only members of staff will be allowed remote access to the shared staff drive. Staff must not allow family members or friends to use the computer while logged in remotely to school resources. They must also not leave the computer unattended while logged in remotely to school resources.

Misuse and Infringements

Complaints

Complaints relating to E-Safety should be made to the E-Safety Coordinator or Head teacher. 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 E-Safety Coordinator.
- 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 E-Safety coordinator, depending on the seriousness of the offence; investigation by the Head teacher, 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 E-Safety 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 E-Safety coordinator.
- 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 as per Child Protection procedures.

Parental Involvement

We believe that it is essential for parents and carers to be fully involved with promoting E-Safety both in and outside of school. We consult and discuss E-Safety 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 E-Safety where appropriate in the form of; Posters, Website and Newsletter items.
- Parents have been informed of the school's approach to E-Safety issues and letters have been sent home informing parents of the SMART rules being taught throughout the curriculum.
- Workshops will be run for parents on a yearly basis to inform them of issues relating to e-safety.

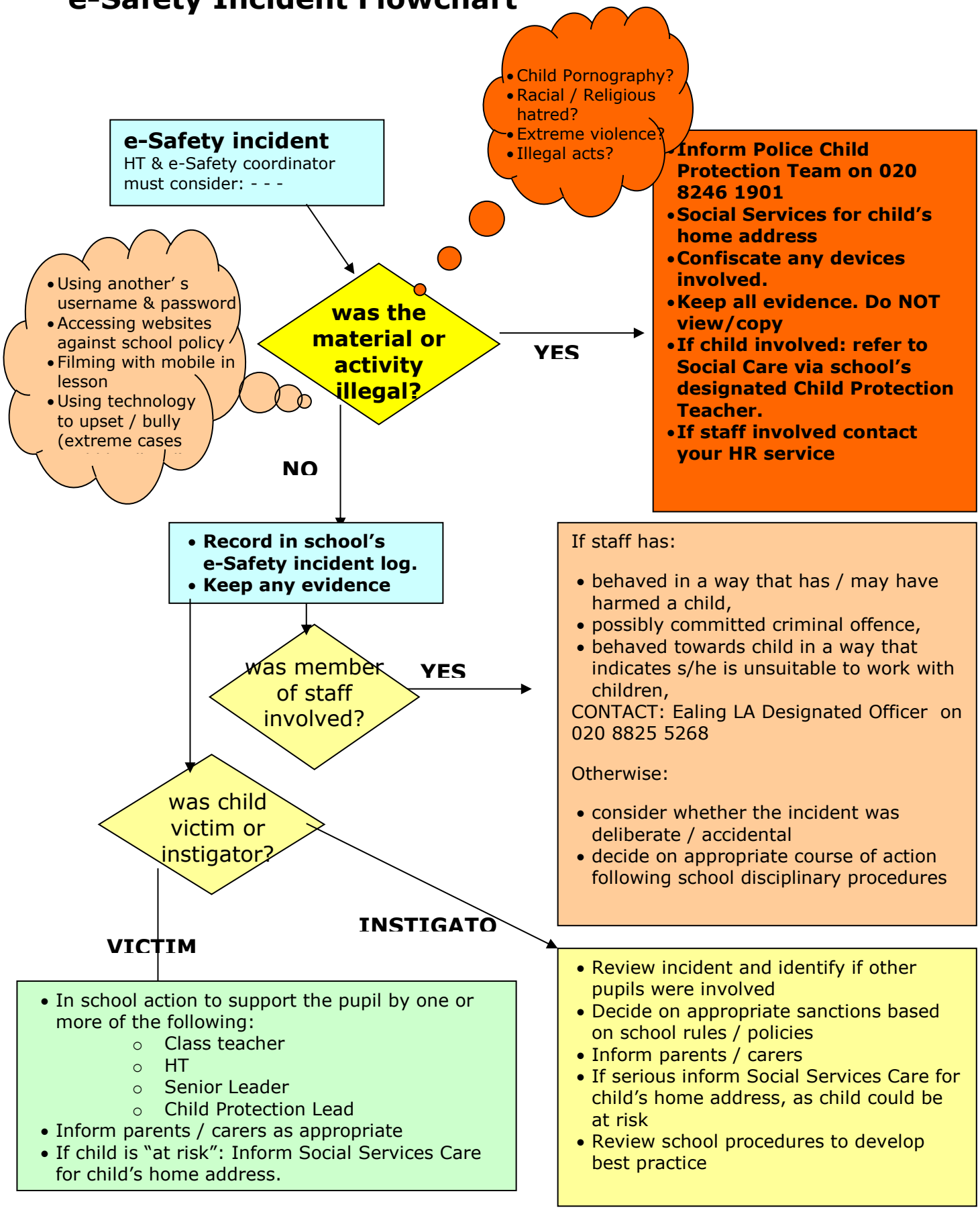
Review Procedure

- There will be an on-going opportunity for staff to discuss with the E-Safety Coordinator any issue of E-Safety that concerns them.
- This policy will be reviewed every 24 months (or sooner if required) 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. E-Safety 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

e-Safety Incident Flowchart



Staff, Governors' and Visitors' Acceptable Use Agreement Form

The school Acceptable Use Policy is designed to ensure that all staff are aware of their responsibilities when using any form of Information & Communications Technology within their professional role.

All staff are expected to sign this policy and adhere at all times to its contents.

- I will comply with the ICT system security protocols and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email/phone accounts/social networking profiles.
- I will not discuss school issues on social networking sites/web-blogs.
- I will not give out my own personal contact details to pupils, such as mobile phone number and personal email address.
- I will only use the approved, secure email system(s) related to my professional role.
- I am aware that communicating with students/pupils via private email/SMS and social networking sites may be considered a disciplinary matter.
- I will ensure that any personal mobile devices are not used or on show in the company of children/pupils.
- 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.
- I will ensure that I only take school personal data off school site in encrypted form, or will access the data remotely.
- I will not install any hardware or software without permission of the Leader of Computing.
- I will not browse, download, upload or distribute any material of a pornographic, offensive, illegal or discriminatory nature. **I understand that to do so may be considered a disciplinary matter, and in some cases a criminal offence.**
- Images & videos of pupils and/or staff will only be taken, stored on school equipment and will only be used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images & video will not be distributed outside the school network / school blog without the permission of the parent/ carer, member of staff or Head teacher.
- 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 or the school 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 have read the full school Acceptable Use Policy and I understand what is expected of me regarding my professional behaviours in the use of technologies.

Signature ……..…… Date ……

Full Name ……..(printed)

Job title . . . . . .

Primary Pupil Acceptable Use

Agreement / E-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT 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 E-Safety.
- ✓ 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 E-Safety 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 Mrs Stubbs (Leader of Computing).

✂----------

Parent/ carer signature

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

Parent/ Carer Signature ……

Class …… Date ……

Beaconsfield Primary E-Safety Incident Log

Details of any incidents relating to E-Safety to be recorded by the E-Safety coordinator. 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 in his absence, Punam Sharma or Tanya Lefort).
- Any incidents relating to cyber bullying should follow bullying policy.
- See E-Safety 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.