West Byfleet Junior School

Online Safety Policy

1.1 - Introduction and purpose

This policy sets out West Byfleet Junior School's commitment to:

- ensure that as far as possible children and their parents are aware of, and equipped to avoid or resist, techniques for the use and abuse of Computing that may adversely affect children's safety or welfare.

This policy applies to all children, parents, staff, visitors, volunteers and contractor who have access to and are users of school digital technology systems both in and out of school, and non-compliance may lead to disciplinary or legal action

1.2 - Context and definitions

This policy follows best practice and is consistent with the requirements and advice of Surrey County Council. It reflects the school's *Values* in general and, in particular, the following:

> *"**Trust***
> *We care about each other and value open and honest communication. Within a physically and emotionally safe environment, we respect the value of risk taking in developing sound judgement. Each can excel and all can celebrate achievements."*
>
> ***"Responsibility***
> *We consider that being involved in, or having access to, education is a privilege, which in return requires each to adopt high standards, act with probity, provide good stewardship of the public assets, deliver value and be fully accountable to all stakeholders."*

This policy is part of the *School Improvement Plan* and relates to the *Computing*, *Anti bullying, Data Protection, Use of Images* policies and *Acceptable Use Agreement*.

1.3 - Overall Responsibilities

The school's Designated Safeguarding Lead (DSL) is aware of e-safety training and resources and is available should any child wish to disclose information regarding an online incident. Therefore it may be good practice to represent an e-safety representative (both pupil and staff). The DSL must be made aware of any disclosures, incidents or child protection concerns. The Senior Management Team (SMT) and Governing Body are involved and should review the e-safety policy and its implementations at least annually or more in the light of significant developments in the use of technologies, new threats to onlinonline safety or incidents that have taken place and monitor its impact. They ensure that they take responsibility for revising the e-safety policy.

The Head-teacher and Governing Body have a legal responsibility to safeguard children and staff and this includes online activity.

1.4 - Why Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The school will, by means of this policy document, set out rules and procedures to be adopted for the provision and use of IT systems and equipment in the school, covering the following: roles and responsibilities; risk assessment and management; teaching and learning; managing internet access; responding to other (and emerging) technologies; managing personal data; ensuring safe and secure systems; and ensuring security of equipment and facilities.

There is also a statement at the end of the document concerning the communication, promulgation and embedding of the policy and procedures, and how complaints should be handled.

1.5 - Roles and responsibilities

The Resources Committee will review and monitor the implementation of this policy and report back to the Full Governing Body on an annual basis as to whether the policy is complied with and what corrective action is required or revisions to policy as appropriate

The school will appoint an E-safety Co-ordinator. The Head teacher will ensure that this policy is implemented.

The school will appoint an IT Support contractor, who will ensure that firewalls, child locks and anti-bullying software protection is installed and maintained. The IT Support contractor will assist the E-safety Co-ordinator in reviewing traffic and isolating cases of abuse of this policy.

All members of staff will maintain vigilance for cases of abuse of this policy and report any instances to the E-safety Co-ordinator.

1.6 – Teaching and learning

Pupils will be taught how to evaluate Internet content and IT processes. Pupils in all year groups will be taught what Internet and IT use is acceptable and what is not, and given clear objectives for Internet and IT use. This will be part of e-safety learning and pupils will be:

- Educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Shown how to publish and present information appropriately to a wider audience.

- Taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Kept safe from terrorist and extremist material on the internet. Pupils will be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues that arise and helping them to understand how they can influence and participate in decision making
- Taught how to report unpleasant Internet and other content. They will report it to the class teacher or TA in charge of the lesson who will inform the E-Safety Co-ordinator who will, in turn, report it to Eduthing (IT Support contractor).

1.7 – E-mail

The school's e-mail system is for use by staff, pupils and governors for school business only:

- pupils must immediately tell a teacher if they receive offensive e-mails
- pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission of the E-safety Co-ordinator.
- Staff to be made aware that email communication may be monitored.

1.8 - Social networking

The school will not allow access to social networking sites through the school's Internet access.
As part of e-safety learning in the curriculum and through parent information evenings, pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

1.9 - How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will carried out (in the form of pre-organised meeting with software consultants) before use in school is allowed.

- Pupils, staff and parents will be instructed about safe and appropriate use of personal devices both on and off site in accordance with appropriate policies.

2.0 - How will published content be managed?

The school website is a good place to display work and experiences and inspires children to engage in their learning. Publication of any information online should always be considered from a personal and school security viewpoint.

Contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information should not be published.

- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

- The school website will comply with the schools guidelines for publications, including respect for intellectual rights, privacy policies and copyrights.

2.1 - Can pupils work be published on the Internet/school website?

Pupils work can add liveliness and interest to a publication either on the schools webpage or on pages created by pupils in accordance with the new primary curriculum. Nevertheless, the security of staff, pupils and parents is paramount. Although common in some forms of media, the publishing of pupils names with certain documents is forbidden and therefore not acceptable. Pupils also need to be taught the reasons for caution in publishing personal information, whether that be at school or at home.

- Images or videos that include pupils or thier work will be selected carefully and will not provide material that could be reused.

- Pupils full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in Surrey Safeguarding Children's Board Guidance on using images of children http://www.surreyscb.org.uk/.

- Written consent will be kept by the school where pupils' images are used for publicity purposes (newspapers, magazines etc.), until the image is no longer in use.

- The school will have a policy in place regarding the use of photographic images of children, which outlines policies and procedures.

2.2 - Communicating and embedding this policy

The success of this policy in safeguarding users will depend on how effectively it is promulgated and embedded in attitudes and behaviour within, and associated with, the school. The school has decided, therefore, that action is taken to maximise the potential impact of the policy as set out in this section of the policy document.

2.3 - Promulgation

The policy will be communicated to children, staff and parents and volunteers on a regular formal basis.

Pupils

The e-safety policy must be introduced to and regularly reinforced with pupils; specifically**:**

- The e-safety policy will be shared with all pupils of the school in the first Computing lesson of each year and when substantial elements of this policy change.
- E-Safety rules will be displayed on opening screen and posted in all networked rooms.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils.

Staff

- In the first INSET day of each academic year, staff will review the e-safety policy and its implementation and agree implementation and any suggested revisions for that academic year.

Parents

Parents' understanding and support is critical:

- Parents' attention will be drawn to the school's e-safety policy in newsletters at least annually, the school brochure and on the school website.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school which acknowledges that they have seen the school e-safety policy and will assist the school in assuring compliance to this policy.

2.4 - How will risks be assessed?

As the quantity and breadth of information through the Internet continues to grow it is not possible to guard against every undesirable situation or content.

- The school will take responsibility precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to un-suitable material will never occur via a school computer. Neither the school nor Surrey County Council (SCC) can accept liability for the material accessed, or any other consequences resulting from Internet use.

- The school and SCC will provide safe and appropriate Internet safeguarding in the form of computer filters and firewalls. The school in accordance with SCC will monitor this on a regular basis to ensure that any websites that previously missed the firewall have been added.

- The school in accordance with SCC will use the ‘RM’ filter system in order to limit the use of inappropriate content from the Internet. However the school cannot guarantee that this filter will block all content and accepts no responsibility if unsuitable material is viewed by accident or through a purposeful violation.

- The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate

- The use of computer systems by whomever, without permission or for inappropriate purposes could constitute a criminal offence under the ‘Computer Misuse Act 1990’ and breaches will be reported to the appropriate authorities.

- Methods to identify, assess and minimise risks will be reviewed regularly.

- Access to school IT systems are controlled by personal passwords for staff.

- Any e-safety incidents will be logged and recorded on CPOMS and discussed with the DSL.

2.5 - Handling e-safety complaints

The school is committed to protecting the security and safety of ICT systems and their users at all times, and believes that prevention measures and routes of redress are important aspects of this commitment. Therefore:

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure
- Pupils and parents will be informed of consequences for pupils misusing the Internet

2.6 - How will cyber-bullying be managed?

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyber-bullying and its effects.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular Section 89 of the 'Education and Inspections Act.'

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents.
- Gives head-teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of the school staff.

Where bullying outside of school (such as online or via text) is reported to the school, it should be investigated and acted on.

- Cyber-bullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- There are clear procedures in place to support anyone in the school community effected by cyber-bullying (refer to DfE: Cyber-bullying advice for head-teachers and school staff).
- All incidents of cyber-bullying are reported to the school and subsequently recorded by the school.
- There are clear procedures in place to investigate incidents or allegations of cyber-bullying.
- Staff/parents and pupils will be asked to keep a record of any cyber-bullying incidents as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses and contacting the service provider and the police if necessary.
- Pupils, parents and staff will be required to work with the school to support the approach to cyber-bullying.
- Should a serious e-safety incident take place the DSL will be advised and the police will be contacted if a criminal offence has been suspected or committed.

2.7 – How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students and staff at specified times in school will be decided by the school according to appropriation.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by a member of the 'Senior Leadership Team' (SLT) with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Staff and visitors to the school must be made aware of the mobile device/phone usage posters around school. This is so they are aware of where they are and are not allowed to use a mobile device. See link for more information: S:\Staffroom\Everyone\COMPUTING\E-Safety

2.8 - Pupils Use of Personal Devices:

- Children may not use personal devices in school; the Headteacher will approve requests to carry a mobile phone to school and all devices must be handed in upon arrival for safekeeping. If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Pupils found in possession of a mobile phone in school will reported to the class teacher.
- During the school day, parents are advised not to contact their child via their mobile phone; but to contact the school office instead.
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

2.9 - Staff Use of Personal Devices:

- Staff are not permitted to use their own personal phones or devices for contacting children, or their families within or outside the setting in a professional capacity unless authorised by the Head/Deputy Head-teacher.
- Staff will use the school office phone where contact with pupils or parent/carers is required.
- Mobile phones and devices will be switched off or put to 'Silent Mode,' Bluetooth communication should be set to invisible/hidden or switched off and mobile phones or devices will not be used during teaching periods for text, calls or e-mails unless authorised by a member of the SMT.
- If members of staff have an educational reason to allow children to use a mobile phone or personal device as part of an educational activity then it will only take place when approved by the SMT.

- Staff should not use their own mobile phone to take photos or videos of pupils and will only use work-permitted/provided equipment for this purpose (school digital camera or an i-Pad).
- Classrooms will be classed as an Amber Mobile Phone Zone where teachers should only be using their mobile device at appropriate specified times: break times, lunch times and after school.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- All staff are required to read, agree to and sign the school's Acceptable Use Agreement.

3.0 – Parental use of personal devices:

- Parents/carers who wish to come into school to help need to attend safeguarding with the Head teacher.
- They must hold a valid DBS Certificate and the school's administration team must confirm this.
- Parents/carers will have to sign and date when they have read the acceptable usage policy for electronic devices within the school.
- Parents/carers will need to view the school's mobile phone heat map to ascertain where mobile device usage is allowed.
- Their mobile device must be switched off when signing in at reception and not be visible to any children.
- Parents/carers are not allowed to use their mobile device if they are working with a child/children.
- Parents/carers must familiarise themselves with the usage heat map and identify the mobile phone zones around school.

3.1 - Home learning and e-safety

- Children to access work via the password protected secure home learning section of the schools website
- Children and adults must be appropriately dressed when attending Zoom conversations
- Staff members should be dressed appropriately during Zoom calls and recordings
- Children must display their face during class registration
- Pupils must report to an adult at home and subsequently to the appropriate staff member if an issue surriounding cyber-bullying takes place
- All children must adhere to the same e-safety guidelines as they would in school, following the SMART way of accessing the Internet
- Parents must have adequate virus protection software on their devices
- Parents must be copied in on e-mails sent from children
- Teachers must copy parents in on e-mails sent directly to a child's e-mail address

- Teachers to follow new e-mail policy regarding protocols when e-mailing parents, remaining professional in tone and content (e.g. the way you address the parents and the e-mail signature).
- Teachers to ensure Zoom calls/recordings take place in a private location within their own homes.
- There should be no background distractions during Zoom calls/recordings.
- Zoom backgrounds should be neutral and not virtual unless otherwise stated.
- Zoom names should be that of the participant/s unless otherwise stated.
- No child should be left on their own in a Zoom conversation. Parents must be able to hear and see the computer screen at all times.
- If a teacher needs to telephone parents from their own personal telephone number, they will ensure the number is withheld.

References:

http://new.surreycc.gov.uk/__data/assets/pdf_file/0005/14558/E-safety-toolkit-for-schools.pdf

http://www.surreycc.gov.uk/__data/assets/pdf_file/0006/650643/NEW-E-Safety-policy-2013.pdf

http://new.surreycc.gov.uk/schools-and-learning/teachers-and-education-staff/educational-advice-and-support-for-teachers/education-safeguarding-in-surrey-schools-and-learning/e-safety-in-education

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf