Bushy Hill Junior School E-safety Policy (2017 review)

Writing and reviewing the E-safety policy

- Also refer to other school policies including: Anti-Bullying, Computing, Child Protection & Safeguarding and Internet Acceptable Use.
- The E-safety coordinators are Louisa Dormer (Head Teacher) and Harry Edward (Computing Lead).
- Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The E-safety Policy and its implementation will be reviewed annually.
- The E-safety Policy was revised by: Harry Edward and Louisa Dormer.
- It was approved by the Governors on: …….

Teaching and Learning

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 recognises its duty to provide students with quality internet access across different digital platforms as part of their learning experience.
- Internet use and the skills required to use the internet effectively are a part of the statutory curriculum for Computing as well as a necessary tool for staff and pupils.
- Through the safe use of digital technologies, all learners will be equipped with the experiences and skills they will use in a rapidly changing technological world.
- E-safety helps to develop the confidence to explore and make use of computing skills to solve problems in all areas of the curriculum.
- The school internet access is provided through a contract with EXA NETWORKS, managed by JSPC. The internet provided features 'Surf Protect' filtering to ensure only age-appropriate material can be accessed on site.

E-Safety embedded in the computing curriculum

- Pupils will be taught by their class teachers what is considered to be acceptable use of digital technologies and what is not. They will be given clear objectives for use of such technologies. They will have at least one e-safety focussed lesson per half term.
- Pupils will be taught to understand computer networks, such as the internet; the range of the services that they provide and the opportunities they offer for communication and collaboration.
- Pupils will be taught to use search technologies effectively, to appreciate how results are selected and ranked, and to be discerning in evaluating digital content.
- Pupils will be equipped with the skill to select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals.
- Pupils will be taught to use digital technologies safely, respectfully and responsibly.
- Pupils will be taught to recognise acceptable/unacceptable behaviour and to identify a range of ways to report concerns about content, contact or conduct.

Staff and pupils will be taught how to understand risks of using digital technologies

- The school recognises that there are three main areas of risk when using digital technologies (including the internet): content, contact and conduct.
    - Content: being exposed to illegal, inappropriate or harmful materials, including material that could be considered to reflect extremist views (see page 6, paragraph 3 -'Radicalisation' as well as the Child Protection and Safeguarding Policy)
    - Contact: being subjected to harmful online interaction with another user or users, regardless of the origin of the contact and whether the user is known to the child or not.
    - Conduct: a child's own personal online behaviour, conduct becomes a risk when it increases the likelihood of (or causes) harm to the child themselves or to others.

- Through this policy as well as the Child Protection and Safeguarding Policy, the school aims to do all it reasonably can to limit children's exposure to harmful materials and ensure pupils will be taught how to report content, contact or conduct that is unwanted, unpleasant or offensive.
- This procedure is as follows:
    - If content or contact is on the screen, turn off the monitor or close the screen of the digital device.
    - Tell an adult about the unwanted, unpleasant or offensive content, contact or conduct.
    - The adult will investigate the child's concerns and follow the procedures set out in Appendix 3 of the Child Protection and Safeguarding Policy.

Staff and pupils will be taught to reflect on and evaluate digital content

- The school will seek to ensure that all use of internet derived materials by staff and by pupils complies with copyright law, and staff and pupils will be taught the need for, and relevance of, these laws.
- Pupils will be taught to be critically aware that any materials they access can come from a wide range of sources and they will be shown different ways that they can validate information before accepting its accuracy.

Managing Internet Access

Authorising internet access for staff, pupils, visitors and the wider community

- All staff must read and sign the Staff Handbook and the 'Staff Code of Conduct' before using any school ICT resource and on receipt of a school email address.
- All pupils must sign the 'Internet Acceptable Use' form alongside their parents before being granted access to the school system and a personal email account.
- The School Business Manager will maintain a record of staff and pupils who are granted access to school ICT systems.
- All use of the school internet connection by the community and external organisations shall be in accordance with the school E-safety Policy.
- All visitors, external organisations and members of the wider community requiring internet access will be required to sign an 'Acceptable Use of School ICT Resources' form before being allowed to access the internet from the school site.
- A list of such authorised users will be stored centrally (in the office) for one year to ensure individuals likely to make a repeat visit (such as a supply teacher) can use the internet again upon returning to the school.
- The Wifi password that guests will use to access the internet will be regularly updated and also stored centrally in the school office for access when necessary.

Information system security

- The security of school systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Strategies will follow guidance from Surrey County Council to meet security requirements.

Email use

- Pupils and staff may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils will be explicitly taught to not reveal any personal details of themselves or others in email communication.
- Pupils will be explicitly taught that they should never arrange to physically meet someone met through the internet without specific permission from a parent/carer.
- Staff to parent email communication must only take place via a school email address or from within the learning platform and should follow acceptable use guidelines.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and should follow acceptable use guidelines.
- SLT will monitor email use as appropriate.
- Incoming emails should be treated with caution; attachments should not be opened unless the author is known and the content appears trustworthy.
- If email contact between pupils and external bodies is deemed appropriate as part of the learning process, class teachers will consider how these messages are presented and controlled.
- The forwarding of chain letters or messages is not permitted.

Published content and the school web site

- The contact details on the school website will be: the school address, email and telephone number. Personal information or contact details for staff or pupils will not be published, beyond current names and roles of members of staff.
- The Head Teacher or an appointed nominee will take overall editorial responsibility to ensure that content is accurate, up-to-date and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published externally.
- All published photographs that include pupils or their work will be selected carefully.
- Photographs of pupils or their work must only be taken using school-owned digital hardware such as a digital camera or tablet.
- Pupils' full names will be avoided in external publications; including in blogs, forums or wikis, particularly in association with photographs.
- Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking

- All social networks, newsgroups and forums will be blocked unless a specific use is approved.
- Pupils will be taught about the age-restrictions on a range of social media and the importance of following such restrictions.
- Pupils will be advised that if they have permission to use social media, to never to give out personal details of any kind which may identify them or their location.
- Pupils will be taught that they must not place personal photos on a social network.
- Pupils will be advised to use nicknames and avatars when using social networks.
- Pupils and parents will be advised that the use of social networks outside school brings a range of dangers for primary aged pupils and due to the age-restrictions may also be illegal in some cases.
- Pupils will be explicitly taught that they should never arrange to physically meet someone met through social media without specific permission from a parent or carer.

Managing filtering

- The school will follow the guidance of the Surrey County Council e-safety toolkit to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to the E-safety Coordinator so this can be reported and filtered.
- Senior staff will ensure that regular checks are made to ensure that filtering methods are appropriate, effective and reasonable.
- While it is essential that appropriate filters and monitoring systems are in place to minimise risks, the school will ensure that it does not "over block" such that there are unreasonable restrictions as to what the children can be taught.

Managing videoconferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised by an adult.

Managing mobile phone technologies

- Children are discouraged to bring mobile phones onto the school premises. If deemed necessary, phones must be handed into the school office at the start of the day and collected at the end.
- Phones (and associated cameras and internet connections) will not be used during lessons or formal school time except as part of a specifically approved educational activity and at the undertaking or a risk assessment.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where external contact with parents or pupils is required.
- Staff will only use mobile phone technologies within the staff room or office.
- Mobile phones must remain switched off elsewhere in the school grounds.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Games machines and consoles such as the Sony Playstation series may have unfiltered internet access. Care will be taken with their use within the school and approval of their use will always be sought from the Head Teacher and a risk assessment undertaken.
- The appropriate use of new Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Permissions

- See page 4 paragraph 1 of this E-Safety Policy for information pertaining to authorised use the school systems and internet by staff, pupils, visitors and other members of the wider community.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed or any consequences of internet access.
- The school will audit the use of digital technologies annually to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Radicalisation

- The school understands that the internet and social media in particular has become a major factor in the radicalisation of young people by terrorist organisations and those seeking to share terrorist ideology and extremist ideas.
- The school understands its responsibility to ensure that children are safe from terrorist and extremist materials and will take all reasonable precautions to prevent online access to such materials through appropriate filtering and monitoring as well as ensuring children know to tell an adult if they encounter inappropriate materials (See section 1 'Teaching and Learning', paragraph 3).
- The school believes it is essential that children are safeguarded from potentially harmful materials and through the E-Safety Policy as well as the Child Protection and Safeguarding policy will do all they reasonably can to limit children's exposure to such materials.
- The school understands the need to assess the risks affecting children and young people in the area and to identify those at risk of radicalisation. See the Child Protection and Safeguarding Policy for further information.

Handling E-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. See Appendix 3 of the Child Protection and Safeguarding Policy – “What to do if you have a concern?”
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the internet.

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils as part of the computing curriculum as well as other lessons featuring use of digital technologies.
- 'Child-friendly' E-safety rules will be posted in all networked rooms.
- Pupils will be informed that network and internet use will be monitored.
- The curriculum ensures regular, explicit teaching of E-safety and the skills required for the safe use of digital technologies.
- Termly assemblies on e-safety will be delivered to both upper and lower school and will be organised by the e-safety leader.

Staff and the E-safety policy

- The importance of the E-safety Policy will be explained to staff, who will sign to show they have read the policy.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff that manage filtering systems or monitor use of digital technologies, including the internet, will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- The school will deliver e-safety workshops and information evenings for parents and carers as needed.

Wi-Fi Access

- See page 4 paragraph 1 of this E-Safety Policy for information pertaining to authorised use the school systems and internet by staff, pupils, visitors and other members of the wider community.