St John's School Billericay

E-Safety Policy including Filtering and Monitoring

Date:	August 2023
Those Responsible:	Mr A Angeli - Headteacher
	Mrs A Fleming – DSL
	Miss B Raynard – E-safety coordinator

E-Safety Policy – Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones, computers and other devices for email, text, instant messaging and social networking. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy should operate in conjunction with other policies including those for Behaviour and Sanctions, Anti-Bullying, Curriculum, Acceptable use of ICT, Safeguarding and Data Protection.

E-Safety depends on effective practice at several levels:

- Responsible ICT use by all staff and students.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems

Roles and Responsibilities

- The school's E-Safety Coordinator is Miss B. Raynard, Deputy DSL. She works in close co-operation with the headteacher, deputy head and safeguarding team to oversee e-safety.
- The proprietor, headteacher and DSL, and the DDSLs are responsible for ensuring that the Filtering and Monitoring standards are met. They ensure that:

- Filtering and monitoring reports are generated and reviewed.
- Safeguarding concerns are acted upon.
- Regular checks are made to the filtering and monitoring systems.
- Reviewing the effectiveness of the provision for filtering and monitoring.

- Day to day management of filtering and monitoring systems requires specialist knowledge of IT staff to be effective. The DSL works closely with the IT Manager to ensure the standards are met. The IT Manager is responsible for:

- Procuring systems
- Carrying out reviews and checks.
- Maintaining filtering and monitoring systems.
- Providing filtering and monitoring reports.
- Completing actions following concerns of checks to systems.

Teaching and learning

Why Internet use is 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 curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Internet areas of risk to focus on

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views
- **Contact :** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and / or financial scams.

Students will be taught how to evaluate Internet content

- Students will be taught in all lessons/form times to be critically aware of the materials / content they access online and are guided to validate the accuracy of information.
- Yearly e-safety sessions are delivered by outside speakers to reinforce pupil's knowledge of potential dangers online.
- A yearly online course for KS3 and KS4 is completed by students to cover risks online, the impact of new technologies on health and relationships.

- Safer Internet Day takes place every February with activities distributed and delivered by every form tutor in the school from Reception to U5 classes.
- Students need to understand the importance of reporting abuse, misuse or access to inappropriate materials. If students (or staff) discover unsuitable sites, the URL (address), time, date and content must be reported to the school E-safety Coordinator.
- Staff should ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Resources to teach online safety could include:

  Be Internet Legend

  Disrepesctnobody

  Education for a connected world framework

  PSHE Association

  Teaching online safety in school

  Thinkuknow

  UK Safer Internet Centre

  National Education Network

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly, at least annually
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

E-mail

- The official school email service may be regarded as safe and secured and is monitored. Students may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- Students must immediately report, to a teacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents/carers must be professional in tone and content.
- Students must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

Publishing pupil's images and work

- Pupils' images will only be used in accordance with the image authorisation form.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked.
- Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Students must not engage in online discussion on personal matters relating to members of the school community.

Students' managing use of personal devices

- Mobile phones/devices will not be used during lessons or any other school time. Form tutors will collect phones at the beginning of the day. The sending of abusive or inappropriate text messages is forbidden.
- If a student breaches the school rules then the phone or device will be confiscated and will be held in a secure place until the end of the day. Repeated breach of school rules may result in phones being handed in to pastoral heads. Parents are informed.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to ask the secretaries in the main school office to phone their parent/carer. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- The recording, taking and sharing of images, video and audio on any student mobile phone is not permitted; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher

is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

Protecting personal data

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

Policy Decisions

Authorising Internet access

- All teaching staff and students are granted Internet access.
- All staff, including Teaching Assistants and Supply Teachers have access to a copy of the E-safety policy and are expected to comply with the acceptable ICT Acceptable User Policy (Staff) when using any school ICT resource.
- Parents of senior pupils and students will be asked to sign the pages in the planner agreeing to comply with the school's Responsible Internet Use Policy.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the Pastoral Heads in consultation with the Deputy Head and the Headteacher.
- If a member of staff is believed to misuse the internet in an abusive or illegal manner, any complaint must be referred to the Headteacher.
- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Parents will be informed of the complaints procedure.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- Mobile phones are not permitted in any of the EYFS classrooms at any time.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not generally use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Where staff are taking groups on school trips, they may take photos of pupils for Facebook or the Website. These should be emailed to a school e-mail address as soon as is practicably possible and then deleted from the staff members' phone. Staff are advised to refer to the media list beforehand and to ensure that they follow safeguarding procedures.

Communications Policy

Introducing the e-safety policy to students

- Rules for Internet access will be posted in all networked rooms.
- Students will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use through PHSE, form times and ICT lessons. Advice could include access to Video Sharing Platforms (eg: TikTok); playing games online and chatting with other members of the online gaming community; being involved in non-contact sexual (ie: watching sexual material); consensual image sharing; harmful online challenges and online hoaxes …

Role of Parents/Carers

- Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. They should be encouraged to monitor their children's online behaviours. As parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet, the school will

take every opportunity to help parents understand these issues through parents' evenings, newsletter/leaflets, website about information about national/local e-safety campaigns / literature.

- Parents and carers will be encouraged to support the school in promoting good e-safety practice and follow guidelines on the appropriate use of digital and video taken at school events and their children's personal devices in the school (where this is allowed).
- Regular communication with parents is maintained throughout the year via emails, documents (from NSPCC, Parent Zone…) sent with termly reports and/or training sessions in order to help them understand the risks of online activities and prevent any major incidents at home. A section of the school website is dedicated to up-to-date E-safety news, which parents can access at any time as well as useful websites: for example Childnet (offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support), Commonsensemedia (provide independent reviews, age ratings, & other information about all types of media for children and their parents), Internet Matters (provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world), Let's Talk About It (provides advice for parents and carers to keep children safe from online radicalisation), National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online, Net-Aware (provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games) ,Parent Info (provides support and guidance for parents from leading experts and organisations), Parentzone (provides help for parents and carers on how to keep their children safe online) , UK Safer Internet Centre (provide tips, advice, guides and other resources to help keep children safe online) and … Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

Staff and E-safety training

All staff can access the E-safety policy via the OneDrive.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

As part of our Safeguarding approach, teaching and supporting staff will be regularly trained to understand e-safety risks and support students with online issues in and out of lessons.

Staff will either attend face-to-face sessions and/or complete an online course (matching the student course offered to KS3 and KS4 students).

Remote learning

Safeguarding approach

We recognise that children are spending longer periods of time online, which may increase their vulnerability. We have provided parents with information on how to keep their children safe online and resources to support them to do this. Particularly useful websites are:

- CEOP (Child Exploitation and Online Protection)
- Childnet
- Internet Matters
- Net Aware
- NSPCC
- Parent Info
- Safer Internet

Staff are aware that children are vulnerable to being bullied or groomed for abuse or radicalisation online. Staff will be vigilant to any signs that that this may be occurring and report any concerns in the usual way.

It is important that parents make the school aware of any concerns they may have about the online activity of their child, or any particular vulnerability they may have in this respect.

Support for children accessible from home

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Filtering and Monitoring

Schools should provide a safe environment to learn and work, including when online. Filtering and Monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. An active and well manged filtering system is an important part of providing a safe environment for pupils to learn.

Filtering

An effective filtering and monitoring system needs to block internet access to harmful sites and inappropriate content. It must be appropriate, effective and reasonable. The filtering is set up for specific user groups e.g teachers and age user groups (Kindergarten pupils, Junior pupils and Senior pupils).

It should **not**:

- Unreasonably impact teaching and learning or school administration.
- Restrict students from learning how to assess and manage risk themselves.

No filtering system can be 100% effective; however, the implementation of this policy ensures that the school filtering system is blocking access to illegal child sexual abuse material, unlawful terrorist content, offensive language and adult content. Staff know how to report and record concerns. Changes and updates are shared with all staff as part of their regular child protection training and as ongoing updates at staff meetings.

Staff know that they should report if:

- They witness or suspect unsuitable material has been accessed.
- They can access unsuitable material.
- They are teaching topics which could create unusual activity on the filtering logs.
- There is failure in the software or abuse of the system.
- There are perceived unreasonable restrictions that affect teaching or administrative tasks.
- They notice abbreviations or misspelling that allow access to restricted material.

Monitoring

It is important that staff are aware that all systems have limitations and know the importance of supervision and monitoring whilst pupils use devices. Monitoring allows schools to review user activity on school devices.

The following strategies are used:

- Staff must be vigilant and take prompt action.
- Physical monitoring by staff watching the screens of users.
- Live supervision by staff on a console with device management software.

Checks to the filtering and monitoring provision are completed and recorded monthly by the IT Manager and shared with the DSL. Block lists are reviewed frequently and can be modified in line with safeguarding risks.

The filtering and monitoring system enables us to identify individuals who might be trying to access unsuitable or illegal material so that they can be supported by appropriate staff, for example, the DSL. We can determine the device used and the individual log in, the time and date of attempted access and the search term or content.

The IT Manager ensures that the filtering and monitoring system works on new devices and services before these are released to staff and pupils. Pupils are not allowed to use their phones to access the interent. This ensures that all cess is via our filtering and monitoring system.