FLASH LEY COMMUNITY PRIMARY SCHOOL

& NURSERY

E – Safety Policy

Flash Ley is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this Commitment.

Produced by: Mrs R Hughes June 2020

Updated by: R. Hughes July 2026

Introduction

Computing and technology is an essential resource to support learning and teaching in an ever evolving digital world, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Flash Ley we need to incorporate the use of technology in order to provide our young people with the skills to access life-long learning and employment.

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks'
(Becta Safeguarding Children Online Feb 2009)

Our E-safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors. The policy will operate in conjunction with other policies including those for computing, bullying, curriculum subjects and safeguarding.

The school's E-safety Co-ordinator & Digital Lead is Mrs. Hughes

The school's Designated Safeguarding Officer is Mrs Banks

Aim

The aim of this policy is to ensure all within the Flash Ley community understand and adhere to effective E-Safety practices, contributing to the protection and safeguarding of all children. This policy outlines the use of technology and how issues which arise with technology use are to be reported and acted upon.

Roles and Responsibilities

Safeguarding is everyone's responsibility and this is applicable to safeguarding children in our technological world. E–Safety is embedded throughout Flash Ley and everyone in the school community plays a role:

Head teacher and Senior Leadership:
The head teacher and senior leadership will ensure that:

- The responsibility of the safety and well-being of all within the Flash Ley community is at the forefront of practice.
- Staff are effectively trained through continual professional development in all aspects of E-Safety to enable them to carry out their E-Safety roles and train other colleagues as relevant.
- Systems are in place to allow for effective monitoring and support for the role undertaken by the E-Safety coordinator.
- Implement policy and procedures that outline how staff use technology in line with the code of conduct.
- E-Safety practices, policies and procedures are regularly reviewed and updated.
- Ensure the DFE filtering and monitoring standards are met.

Teachers and School Staff:
Teachers and teaching staff play a pivotal role in safeguarding children; this includes in the use of technology. Teachers and teaching staff will ensure:

- Teach E-Safety thoroughly through both the computing and PSHE/RSE curriculum ensuring children's understanding is proficient.
- The use of technology, including the internet, for teaching and learning purposes is researched and suitable for the age group of the children who access it.
- Remind children at all times of E-Safety expectations and the role they play in protecting themselves and others including what they should do if they see something they feel isn't right.
- Report any E-Safety issues immediately as they arise via the designated school E-Safety email: esafety@flashley.staffs.sch.uk See section: Handling E-Safety.
- Read, understand and adhere to the whole school E-Safety policy and related policies: bullying, safeguarding, computing, mobile phone, smart technology, media communications and acceptable use.
- Provide a positive role model for children at all times. This includes adhering to the staff code of conduct in relation to staff use of technology both in school and beyond.

The Digital Lead
Flash Ley understands the importance of E-Safety and has a designated E-Safety/Digital Lead. This person will ensure:

- Staff read, understand and adhere to the whole school E-Safety policy and related policies: bullying, safeguarding, computing, mobile phone, media communications and acceptable use.
- Effective E-Safety policies and documents are implemented and reviewed regularly, updating where required.
- All E-Safety issues are reported, recorded and acted upon in a timely manner, providing evidence of actions and resolutions
- E-Safety is taught throughout the computing curriculum and reinforced through daily

teaching and cross curricular links to PSHE/RSE.

- Parents and Carers are informed, supported and guided in navigating E-safety beyond school. This may include sharing information, links to apps and suggested E-Safety practices in the home. At all times Parents will be encouraged to share E-Safety concerns and seek support and guidance where required from the E-Safety coordinator and school staff.
- Filtering and monitoring procedures are effective.

Children:

At Flash Ley our children are taught E-safety and their responsibility to protect themselves and others through a broad and varied computing curriculum. Children access technology across all aspects of the curriculum and are expected to apply their E-Safety knowledge at all times. Children are expected to follow E-Safety practices which protect their online safety:

- Only open webpages as instructed by Staff.
- Children understand that their technology use in school is monitored and accessing or attempting to access filtered/restricted or inappropriate content is dealt with in line with the schools behavior policy.
- Report to staff anything they may see which makes them feel uncomfortable, unsure or scared both within school or at home including webpages, apps and communication.
- When using communication via technology children are to ensure they are kind, polite and understand bullying through the means of technology will be addressed in line with the school bullying policy.
- Children apply their learning of E-Safety to safe practices including but not limited to never sharing passwords or personal information online.
- Children agree not to upload, share or distribute any images of themselves online within school and apply E-Safety practices in the home.
- Never meet a stranger and always tell an adult if a stranger online suggests meeting in person.
- Children agree to adhere to rules relating to copyright and privacy, not using one another's work, accessing others information or sharing content which was not created by them.

Teaching & Learning

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

- The computing curriculum incorporates E-Safety and digital literacy and links to PSHE/RSE curriculums to provide children with all the necessary skills to safely progress in a digital world.
- School internet access will be designed for safe and secure pupil use and the use of content filtering will be embedded into the schools internet system. Filtering and monitoring systems are in place to ensure children are protected from inappropriate content. These are regularly recorded and reviewed.
- Children are given clear objectives within learning whilst accessing technology. Children who are found to deviate from the teaching instruction given may be removed from a computer.
- The school will ensure all children access technology regardless of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances.

E-Safety Aspects

Flash Ley understands E-Safety is a broad and ever changing subject. The below information is not a definitive list of all scenarios but outlines how our school community is protected in our everyday use of technology.

Protecting Personal Data:
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

Internet Use:
The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- Content filtering is enabled at all times; this can be updated regularly should staff become aware of words or phrases which require filtering. All changes are recorded in the filtering and monitoring folder.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible and virus protection is kept up to date.
- Staff are aware of and adhere to reporting E-Safety issues as outlined in the following section 'Handling E-Safety'.
- Children will be educated in safe internet use and how to safely access, retrieve and evaluate information online.
- Children will be taught to be critically aware of materials and content found online and guided into validating the accuracy of information they acquire.
- The school will ensure internet derived materials comply with copyright law.
- Children will be educated in how to ensure they are safe and secure online including privacy and security, copyright and ownership and managing online information.
- The use of YouTube is strictly prohibited during children's free choice time. YouTube is to be accessed as a teaching tool only by staff and no child should access YouTube without the supervision of an adult.
- When technology is in use by children recreationally, the guided access option must be utilized by staff to ensure children's access to apps is limited to those pre-approved by an adult.

Email:
E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage at Flash Ley is an important part of E-Safety:

- Children do not use E-mail in school to communicate with one another or adults.
- Access in school to external personal e-mail accounts is restricted.
- E-mails sent to external organisations should be written carefully and email addresses checked.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.
- Staff will only use their own staff email for work purposes and no personal email account will be used to discuss work related matters.
- Confidential or sensitive documentations is encrypted to ensure maximum safety and security.

Privacy & Security:
Passwords and security play a crucial role in the safety of our school community. Flash Ley will ensure:

- Children are educated on the importance of keeping passwords and personal information private.
- Passwords for staff to access systems and emails are updated regularly.
- In Key Stage 1 and 2 children use their own school login details to access technology. Staff are not permitted to share or allow children to use their log in details.

Social Networking:
Flash Ley recognises the popularity of Social networking in today's world. However, Social networking sites provide facilities to communicate and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact. Therefore at Flash Ley:

- Use of social networking sites and newsgroups in the school, is prohibited and social networking sites and affiliates are filtered.
- Children and Parents/Carers are advised and educated on age restrictions, safety issues and safe use of social networks. Children are reminded of E-Safety practices should they use these beyond school.
- Children are not permitted to upload to social media outside school any content which may identify the school or personal details related to the school such as the location.
- Parents will be informed of and information provided on social networking sites regularly to support them in continuing the school E-Safety practices in the home.
- The school will act upon all forms of bullying in line with bullying policy, this includes bullying that occurs via social media platforms.
- Staff are not permitted to befriend/contact Parents/Carers via personal social media channels.
- Staff are advised to use a variation of their full name on personal social media platforms to limit being identified by Parents/Carers.

Published Content/School Website/Social Media:
The school website, social media channels and app are a valuable source of information for Parents and Carers. Whilst utilising this technology Flash Ley will ensure:

- Contact details on the Website/Social media channels/App will be the school address, e-mail and telephone number. Staff and pupils' personal information will not be published.
- Staff details will only include surnames without forenames or photographs to limit personal exposure.
- The Head teacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos published to the school social media sites and the school website will not include the faces of any children or photographs in which children are identifiable. Only photographs of activities, resources and unidentifiable body parts will be published such as hands.
- Pupils' full names will not be used in association with photographs.
- Consent from Parents will be obtained before photographs of pupils are published on the school website/social media channels on registration. It is the responsibility fo the Parents/Carers to update these preferences should they change.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child/children onto their own social networking site or our social media channels. Parents/Carers are not able to post

onto any school platform.
- The Governing body may ban the use of photographic equipment by any parent who does not adhere to school policy.

Mobile Phones/Smart Technology:

Many new mobile phones have access to the internet alongside picture and video functions. Smart technology, such as smart watches, also present features which pose a risk to children's digital safety. These features allow opportunities for unrestricted access to the internet and sharing of images. There are risks of cyber bullying, or inappropriate contact. Therefore:

- Pupils are advised not to bring mobile phones onto the school site, however if Parents have requested they have one these are kept in designated classroom storage units.
- The sending of abusive or inappropriate text messages is forbidden and bullying via mobile phones will be dealt with in accordance to the school bullying policy.
- Staff should always use the school phone to contact Parents. Personal mobiles are not to be used unless in an emergency (i.e. no school phone connection, emergency use on a trip).
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom/one of the school offices.
- Staff are
- Parents/Carers cannot use mobile phones on site to take pictures, record videos or share content. This applies to event days and Parents/Carers may be asked to delete any photographs/videos taken on school site.
- Smart watches and fitbits are permitted to be worn by staff but to be used only as a watch when working with children. Other functions must be disabled via the use of areoplane mode or limits of other functions. Smart technology must remain on silent mode to eradicate distractions.
- Pupils are not permitted to wear smart watches or other wearable technology devices in school.

See Mobile Phone Policy

Artificial Intelligence

We recognize Artificial Intelligence is a fast-growing part of our digital world, however we also understand the limitations of AI and the risks associated with a newly developing concept. Within our computing curriculum and PSHE lessons E-Safety and digital literacy is taught from Early Years to ensure children understand how to safeguard themselves and others. In Year 6 a unit dedicated to Artificial Intelligence is taught.

As a school we:

- Filter the use of AI for all pupils with the exception of year 6 within the teaching of their computing unit. This decision will be revisited as AI develops in it's reliability and safety but at this moment in time AI presents to many risks and limitations to high quality teaching to be incorporated pupil's everyday use.
- Staff may access the use of AI to support with lesson planning and resourcing in keeping with professional integrity and acceptable use.
- Teachers are responsible for verifying the accuracy and suitability of AI supported resources.
- AI generated work must be referenced where required.
- No AI tool is to used for assessment purposes or to mark tasks.

Digital/Video Cameras/Photographs:
Pictures, videos and sound are not directly connected to the Internet but images are easily transferred. At Flash Ley to safeguard our school community we will ensure:

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff. Where Ipads are being used, children are forbidden to upload any videos/pictures/content unless given permission to do so by the teacher.
- Publishing of images, video and sound will follow the policy set out in this document under 'Published Content'.
- Parents and Carers are not permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites.
- The Head teachers or a nominee may in some cases inform Parents/Carers present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- Staff should always use a school camera to capture images and should not use their personal devices.
- EYFS staff who take pictures of children readily do so with a clear objective and purpose. EYFS have dedicated Ipads which are kept in the room at all times and not taken off school premises.
- Photos taken by the school are subject to the Data Protection act.
- All photos, videos and sound recordings of children are kept on school premises, on school devices that are password protected.
- IPads are linked to the schools filtering and monitoring systems.

Sexting:
'Sexting' is the act of sending sexually explicit photographs, primarily between mobile phones but also using the Internet. All incidents of 'sexting' will be reported by staff to the E-Safety coordinator and Designated Safeguarding Lead. To protect our school community from sexting Flash ley will ensure:

- The use of the internet is restricted within school and access to inappropriate websites is blocked. If under the age of 18, it is a violation of UK law to distribute sexually explicit pictures of you or another.
- If children engage in sexting with a friend, boyfriend, or girlfriend or other party, all involved could find themselves in trouble with the law.
- If a child discloses to staff they have been involved in sexting or a staff member becomes aware of sexting they must report it immediately to the designated safeguarding lead.
- Together with the designated safeguarding lead sexting incidents must be recorded along with the actions to be taken.
- The reporting adult must try to find out what is included – images, video or text messaging, who sent it, who has received it, who is featured if more than one person, if this is a school or personal device and how the child is feeling.
- Never view any images. If these are present on school devices they must be isolated. This may involve blocking the network to all users temporarily.
- Copying, printing or sharing of images is prohibited, unless a safeguarding action requires this (i.e police involvement).

If the sexting incident was not intended to cause harm and the children involved had given consent it is down to the designated safeguarding lead to agree on course of action. However a child protection referral must be made if the following occurs:

- There is any adult involvement
- It is suspected coercion or blackmail has occurred
- The images are extreme or violent in nature
- The child involved in identified as vulnerable
- Any children involved are under the age of 13
- There is deemed a significant risk of harm to a child

See: Safeguarding Policy

Grooming:
It is now a criminal offence for anyone aged 18 or over to intentionally communicate with a child under 16, where the person acts for a sexual purpose and the communication is sexual or intended to elicit a sexual response. This is known collectively as 'grooming'. At Flash Ley staff will ensure:

- Grooming offences apply to online and offline communication and staff understand this may occur via social media, email, text messaging, lettrs and verbally.
- Where staff are concerned communication between children and others is inappropriate this is reported to the schools designated safeguarding lead.
- Concerns are recorded and acted upon in line with school policy.

See: Safeguarding Policy

Assessing Risk
We at Flash Ley understand that in today's world children need to access, understand and be able to utilize technology. However we are aware of the risks this poses and aim to minimise children's exposure to risk through:

- Taking all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Should unsuitable material arise it is immediately reported via the schools designated E-Safety email and dealt with accordingly.
- Regularly monitoring and assessing E-Safety practices.
- Our curriculum is devised using the demographic of our pupils and filtering systems ensure children are protected from inappropriate content but also provide a balance in the quality of teaching and learning some sensitive topics in which resource dsmay need to be presented by teaching staff. Age-appropriate filtering is devised for varying ages of children i.e. Key stage 1 and 2.
- The school does not accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

Handling E-Safety

It is the responsibility of the whole school community to handle E-safety concerns, issues and complaints effectively. Where required school staff are supported in dealing with and resolving any concerns and issues as they arise by the Head teacher, Designated Safeguarding Lead and E-Safety coordinator. The following procedure ensures E-Safety concerns are reported, recorded and acted upon. Flash Ley will adopt an 'if in doubt report it' ethos. E-Safety concerns to be reported are listed as but not limited to:

- Unacceptable internet use by children and school staff.
- Inappropriate content that appears unfiltered through the system.
- Any use of technology which becomes frequent within peers groups such as popular

apps, games or websites in which staff feel children, Parents and Carers may need information, advice or guidance on.
- Taking, sharing or uploading of images, video or sound recording within school beyond teaching and learning instructions.
- The use of mobile phones that does not fall in line with the school mobile phone policy.
- Content which children found upsetting or uncomfortable.
- Concerns shared by Parents and Carers or where Parents and Carers seek advice on any element of E-Safety beyond school.

Reporting concerns and issues must follow the below procedure:
- Staff must immediately record and share the concern with the E-Safety coordinator via the designated email: esafety@flashley.staffs.sch.uk including specific details of the concern or issue, for example the website accessed, inappropriate content viewed etc.
- The E-Safety coordinator will respond in a timely manner with suggested actions which then must be carried out by the staff member.
- Where required the E-Safety coordinator will share concerns with Designated safeguarding leads, the Head teacher or staff on a 'need to know basis'.
- Where concerns maybe applicable to all children, the E-Safety coordinator will provide all staff with information, advice and guidance.
- Where required the E-Safety coordinator will provide Parents and Carers with information, guidance and advice.
- Issues which arise that include child protection will be forwarded to the designated safeguarding lead and dealt with in line with further school policy such as safeguarding and bullying policies.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Prevent Statement

At Flash Ley, Nursery and Voyage provision we aim to prepare our students to become good citizens of the future. Through our curriculum we teach pupils British values and how to celebrate diversity. We aim to raise awareness of radicalisation and extremist views, whatever the source. We have adopted the principles and advice found in 'Keeping Children Safe in Education 2015' and the 'Prevent Strategy 2011'. These are incorporated into our school policy on tackling extremism. E-Safety plays a crucial part in tackling radicalisation as outlined in this policy to protect children when they see something online they find upsetting and how they ensure their own personal online safety.

Links to School Policy

The E-Safety Policy is implemented in line with supporting school policies. Any of these policies may be used to implement procedures related to E-Safety where required:
- Safeguarding Policy
- Bullying Policy
- Computing Policy
- Mobile Phone policy
- Filtering and Monitoring policy
- Acceptable Use Policy
- Media Communications Policy
- Staff Code of Conduct

ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.