



# St. Stephen's School and Children's Centre

*Learning for Life*

## Federated Online Safety Policy

This policy will be reviewed every 2 years

	<b>Date</b>	<b>By</b>	<b>Role</b>	<b>Ratified</b>	<b>Date</b>
Version 4	January 2018	Esther Williams	Online Safety Coordinator	Governing Body	Feb 2017
Version 5	June 2019	Adam Bennett	Online Safety Coordinator	Governing Body	June 2019
Version 6	June 2020	Rebekah Finlay	Online Safety Coordinator	Governing Body	June 2020
Version 7	November 2020	Eva Duncan	Online Safety Coordinator	Governing Body	Nov 2020
Version 8	November 2022	Shabana Zia James Frecknall	Online Safety Coordinator DSL	Governing Body	Dec 2022
Version 9	April 2025	Shabana Zia Rebekah Finlay	Computing Lead AHT - DSL Online Safety	Governing Body	July 2025



St. Stephen's School  
and Children's Centre  
*Learning for life*

Article 17

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

Contents

- **Section 1: Computing in the National Curriculum**
- **Section 2: Context**
- **Section 3: Roles and Responsibilities**
- **Section 4: Education and Curriculum**
- **Section 5: Communications**
- **Section 6: How will complaints regarding Online safety be handled?**
- **Section 7: Technical and Infrastructure**

Our Online Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been agreed by the Senior Leadership Team and approved by Governors.

This policy applies to all members of the St Stephen's Primary School community (including teaching, supply and support staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

## **1. Computing in the National Curriculum:**

The Government has incorporated Online safety into the Computing Curriculum in the following statements:

### **Introduction**

Computing ensures that pupils become digitally literate - able to use, and express themselves through, information and communication technology - at a level suitable for the future workplace and as active participants in a digital world.

### **Aims**

The National Curriculum for Computing aims to ensure that all pupils:

- are responsible, competent, confident and creative users of information and communication technology.

### **Early Years and Key Stage 1**

Age appropriately, pupils should be taught to:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

### **Key Stage 2**

Pupils should be taught to:

- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

It is clear that digital technology provides many educational opportunities but is not without its risks. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually. We also know that computing and technology can offer new weapons for bullies, who may torment their victims via websites or text messages. On top of all this is the ever-present risk that children and young people may be exposed to inappropriate content when online and the potential results of this are yet to be fully understood.

At St. Stephen's, we recognise that it is our duty to ensure that every child in our care is safe and the same principles and ethics should apply to the 'virtual' or digital world as would be applied to the school's physical buildings. However, we also believe that our duty of care extends beyond the physical boundaries of the school and so aim to equip our students with the understanding and skills they need to negotiate the digital world safely at all times. It is the responsibility of all staff at the school to address the issues associated with the online world, ensuring all children are using online devices safely and securely.

This Policy document is drawn up to protect all parties: the students, their families, the school and its staff. It aims to provide clear advice and guidance on how to minimise risks and deal with issues whilst developing awareness and resilience in our pupils and their families.

Online Safety is also embedded within the Federation's Relationships and Health Education (RHE) policy, ratified following consultation in Spring 2021. This policy should be read alongside the RHE policy.

## 2. **Context**

Computing in the 21<sup>st</sup> Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include, but are not limited to:

- The Internet & Website use
- E-mail
- Instant messaging often using simple web cams
- Blogs
- Podcasts
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Games consoles, including those with internet functionality
- Smartphones with full internet capability

It is essential that all teachers are aware of the technologies that children are using both inside and outside school. This awareness can be achieved through the following:

- regular discussions in class about the use of technologies
- being clear that there is a 'no blame' cultures for anyone who has had a bad experience
- zero-tolerance of any form of bullying
- reinforcement of key messages:
  - Zip it, block it, flag it.
  - Keep adults informed of what you are doing online.

Creating a safe Online technology learning environment includes four main elements at this school:

- Technological tools that are well-managed with regular security updates, browser settings and a firewall set to enhanced protection. Google Safesearch is enabled.
- Policies and procedures, with clear roles and responsibilities;
- An effective Online Safety education programme for pupils, staff (and parents where possible).
- A 'no blame' culture in which issues can be openly discussed.

### **3. Roles and responsibilities**

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy is monitored. The responsibility for Online Safety has been designated to a member of the senior leadership team.

The Designated Safeguarding Lead and Online Safety Coordinator ensure that they keep up to date with Online Safety issues and guidance through liaison with the Local Authority Online Safety Officer and through organisations, such as Becta and The Child Exploitation and Online Protection (CEOP). The Designated Safeguarding Lead ensures the Head, senior leaders and Governors are updated as necessary.

Governors need to have an overview of understanding Online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the school's policy on key areas including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- their role in providing Online Safety education for pupils;

Staff are reminded / updated about Online Safety matters at least once a year.

Online safety is included in the curriculum to ensure that every pupil has been educated about safe and responsible use, including how to control and minimise online risks and how to report a problem.

Regular Online Safety Workshops are held for parents/guardians/carers in order to discuss Online safety matters and they have signed and returned Online safety/AUP forms.

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

#### **4. Education & Curriculum**

St Stephen's Primary School acknowledges both the risks and significant benefits of children being online. Recognising technology as a vital part of modern life, the school is committed to helping pupils develop essential digital skills. The integration of technology in education is guided by pedagogical aims and a focus on inclusion.

A structured, age-appropriate online safety curriculum is delivered across subjects, especially in RSHE/PSHE, Computing, and Citizenship, with emphasis on developing competencies, not just risk awareness. The school follows a whole-school approach to embed online safety, including staff responsibilities to incorporate it across the curriculum and in everyday school life.

Students will be taught about online safety as part of the curriculum.

In **Key Stage 1**, students will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Key Stage 2**, students will be taught to:

- Use technology safely, respectfully, and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

Online safety is embedded within computing lessons taught by the school's **Computing Specialist Teacher**, who has been at St Stephen's since 2019. This teacher delivers online safety content to all year groups from **Reception to Year 6**, ensuring progression and consistency across the school. Additionally the school has an assigned Assistant Headteacher who is also responsible and oversees safeguarding concerns regarding online safety behaviour.

Key tools and frameworks used include:

- **LGfL's SafeSkills Quiz and Diagnostic Tool** for ongoing assessment
- **UKCIS 'Education for a Connected World - 2020'** framework
- **Kapow subscription resources** tailored to student needs
- **Annual curriculum reviews and online safety audits**, ensuring alignment with national guidance and SEND considerations

All staff are expected to monitor online use, support safe behaviour, and teach digital literacy skills such as evaluating online content, using generative AI responsibly, and understanding legal issues like copyright and data protection.

**Note:** The RSHE curriculum may change significantly in 2024-25 following a national consultation.

## **5. Communications**

### ***How will the policy be introduced to pupils?***

Many pupils are very familiar with the culture of new technologies and may have encountered Online safety issues themselves. However, pupils' perceptions of the risks involved may not be mature or the concepts may appear abstract at first. For this reason, Online safety rules should be introduced in the context of real life experiences. The school has developed a sequence of lessons that are delivered throughout the year that begin with children's experiences and utilise some of the excellent resources that exist, including:

- Kapow Online Education Units of work
- Think U Know ([www.thinkuknow.co.uk](http://www.thinkuknow.co.uk))
- Googles' Be Internet Legends

As with all areas of the St. Stephen's curriculum, there is no 'one size' fits all programme of study and all units are adapted to be age and stage appropriate to our pupils.

The online resources at our disposal are constantly changing and the Computing and Online safety team at NPW (Newham Partnership Working) keep us up-to-date with developments through our MLE (Managed Learning Environment) and regular network meetings.

Further Online safety education is delivered through leadership assemblies and through PSHE lessons and discussions.

### ***How will the policy be discussed with staff?***

It is important that all staff feel confident to use new technologies in teaching. Staff are given regular opportunities to discuss the issues and develop appropriate teaching strategies. Staff receive online safety training annually.

If a member of staff is concerned about any aspect of their Computing use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

Computing use is widespread and all staff including administration, caretaker, governors and helpers will be included in appropriate awareness raising and training. Induction of new staff will include a discussion of the school's Online safety Policy.

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor Computing use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy

Staff Acceptable Use Policy

[KS1 Acceptable Use Policy](#)

[KS2 Acceptable Use Policy](#) - As of September 2024, we set the policy on a Google form for children to complete.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place.

Further to these steps, the school reserves the right to withdraw - temporarily or permanently - any or all access to such technology, or the right to bring devices onto school property.

### ***How will parents' support be enlisted?***

Internet use in pupils' homes is increasing rapidly and unless parents are aware of the dangers, pupils may have unrestricted access to the Internet.

St. Stephens strives to help parents plan appropriate supervised use of the Internet at home. This is done through:

- Suggested online activities through the Headteacher's Newsletter and a termly Online Safety Newsletter which can be found on the school website for parents to access.
- A section of useful web links for parents on the school website.
- All weekly homework sheets include an online safety reminder for parents as well as age-related screen time recommendations.
- Informing parents immediately of any concerns regarding any individual's use of technology.
- Online safety training for parents.
- Inclusion of online safety content in 'Meet the Teacher' workshops.

### **6. How will complaints regarding Online Safety be handled?**

The school and local authority will take all reasonable precautions to ensure that risks are kept to a minimum through strict systems of filtering content and monitoring activity. However, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. Any inappropriate material is reported to the local authority for them to block. Pupil chromebooks have a key on the keyboard to lock their screens.

Staff and pupils are aware of infringements and the possible sanctions attached. Sanctions available include:

- interview/counselling by Learning Mentor / Class Teacher / Head of Key Stage / Online safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- referral to LA / Police.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

St Stephen's Primary School is committed to safeguarding pupils online and takes all reasonable precautions to prevent harm. However, it acknowledges that online incidents can occur both in and outside of school and may continue to affect pupils during school time or prolonged absences.

All members of the school community are encouraged to report online safety concerns promptly. Any suspected online risk or incident must be reported to the Designated Safeguarding Lead (DSL) on the same day and logged using the school's online Wellbeing Reporting System. Concerns raised by filtering and monitoring systems must also be reported this way.

If an allegation involves a member of staff, it must be reported directly to the Headteacher. If the concern is about the Headteacher, it should go to the Chair of Governors and the Local Authority Designated Officer (LADO). Staff can also contact the NSPCC Whistleblowing Helpline.

The school works with relevant external agencies such as the local authority, LGfL, UK Safer Internet Centre, CEOP, Prevent, Police, IWF, and others for support with serious incidents.

In line with DfE Behaviour in Schools (2024) guidance, the school follows proper procedures for addressing online behaviour issues, including peer-on-peer abuse, mobile phone misuse, and online sexual harassment (see pages 31-33 of the guidance).

Parents/carers will be informed of online incidents involving their child. Where necessary, the Police will also be notified. The school ensures that online safety procedures are robust and sustainable during any unexpected school closures.

## **7. Technical and Infrastructure**

### **The borough**

- Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- Ensures their network is 'healthy' by having LA or Synetrix health checks annually on the network;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
- Provides a filtering service which prevents pupils and staff from accessing inappropriate websites or content e.g. facebook and other social media platforms.

### **St. Stephen's Primary School**

- Works in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Has additional user-level filtering in-place using the *Synetrix USO service*.
- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Use of the lock key on chromebooks to freeze screens.
- Uses individual log-ins for pupils from reception and all other users;
- Uses security time-outs on Internet access where practicable / useful;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses Google Safe Search to limit the possibility of pupils accessing inappropriate material;
- Ensures pupils only publish within appropriately secure learning environments (London MLE).

### **Policy and procedures**

#### **St. Stephen's Primary School**

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview all sites before use or only use sites accessed from managed 'safe' environments such as the Learning Platform;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Never allows pupils to conduct 'raw' image searches e.g. Google or image search;
- Informs users that Internet use is monitored;
- Informs staff and students that they must report any failure of the filtering systems directly to the Child Protection/Online safety Coordinator. Our systems administrators report to LA / LGfL where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses LGfL for pupil's own online creative areas;
- Has blocked pupil access to music download or shopping sites - except those approved for educational purposes such as LGfL's Audio Network;

- Requires pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an Online safety / acceptable use agreement form, including consent to use the internet, which is fully explained and used as part of the teaching programme;
- Uses closed / simulated environments for e-mail with Key Stage 2 pupils;
- Requires all staff to sign an Online safety / acceptable use agreement form and keeps a copy on file in the Single Central Record File and makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities - Police - and the LA.

## **Education and training**

### **St. Stephen's Primary School**

- Ensures pupils know what to do if they find inappropriate web material i.e. use the lock key, and report the incident to the teacher immediately.
- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable, including cyber-bullying incidents.
- Ensures staff report all incidents listed above to Online safety coordinator;
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- Ensures staff understand data protection and general Computing security issues linked to their role and responsibilities;
- Runs a rolling programme of advice, guidance and training for parents, including: Information leaflets in school newsletters and on the school website and on weekly homework sheets, distribution of 'think u know' for parents materials, demonstrations and practical sessions held at school.
- Has a clear, progressive Online safety education programme built on national guidance teaching a range of skills and behaviours appropriate to their age and experience:

#### **INTERNET SEARCHING**

- To STOP and THINK before they CLICK
- To develop a range of strategies to validate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- To know how to narrow down or refine a search;
- To know not to download any files - such as music files - without permission;

#### **ON-LINE COMMUNICATION**

- To understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour.
- To never delete or respond to malicious or threatening emails or messages and show them to a responsible adult;
- To get teacher approval before contacting external organisations or individuals;
- To get teacher approval before opening or sending attachments;
- To never embed information e.g. adverts, images;
- To understand why on-line 'friends' may not be who they say they are;
- To never arrange to meet anyone they meet online without having discussed it with an adult and to never meet anyone you have met online without a responsible adult present;
- To never forward chain email letters or open an email from an unknown sender;
- To have strategies for dealing with receipt of inappropriate materials;
- Pupils are encouraged to invite known friends only and deny access to others.

#### □ PROTECTION OF PRIVACY

- To never give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- To never place personal photos on any social network platforms due its public nature. Advice will include reference to background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- To understand why they must not post pictures or videos of others without their permission;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, personal thoughts, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To set passwords, deny access to unknown individuals and block unwanted communications.

### **MANAGING EMAIL**

#### **At St. Stephens Primary School**

- We do not publish personal email addresses of pupils or staff (Except for Members of the Senior Leadership Team) on the school website. We use [info@st-stephens.newham.sch.uk](mailto:info@st-stephens.newham.sch.uk) for communication with the wider public.
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the Police.
- Accounts are managed effectively, with up to date account details of users.
- Messages relating to or in support of illegal activities will be reported to the relevant Authority and Police.
- We use the Local Authority / LGfL anti-virus product Sophos and additional email, spam, phishing software provided by our LA .

#### **For pupils**

- We do not use email that identifies the name and school of the pupil.
- Pupils can only use the LGfL / school domain email accounts on the school system.
- Pupils are introduced to, and use email as part of the Computing scheme of work.

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and more generally, for example personal accounts set-up at home. See SECTION 1 - Education and training for more details.

#### **For staff**

- Staff use LGfL e-mail system for professional purposes;
- Staff are allowed to only use the LGfL / school domain email accounts on the school system and we do not allow staff to access personal email during the school day;
- We have a 'closed' LA secure email system which is used for some 'LA approved' transfers of information we consider to be sensitive (some protect-level data);
- Staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper, and should follow these guidelines:
  - That it should follow the school 'house-style';
  - The sending of multiple or large attachments should be limited;
  - Personal information must not be sent as attachments on open email. A secure method of encrypted transfer should always be used;
  - The sending of chain letters is not permitted;
  - Embedding adverts is not allowed;

### **USE OF DIGITAL AND VIDEO IMAGES**

#### **At St. Stephens Primary School**

- The Designated Safeguarding Lead takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to School -Based Technician, Designated Safeguarding Lead and Computing Coordinator.
- The school website complies with the school's 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, email address and telephone number.
- Photographs of pupils published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child at the beginning of every school year.
- Digital images /video of pupils are stored on Google Photos, part of Google Workspace, and are deleted at the end of the school year - unless an item is specifically kept for a school purpose;
- When publishing to the school website we do not use pupils' names in the file titles or <ALT> tags of images;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff are not allowed to use mobile phones / personal equipment for taking pictures of pupils as stated in the school's Acceptable Use Policy signed by all staff;
- Pupils are taught about how images can be abused in their Online safety education programme;

#### **Social networking and personal publishing at St. Stephen's**

- The LA blocks access to all social networking sites in school;
- Newsgroups/forums will be blocked unless a specific use is approved by the Online safety coordinator;

- Actively advises parents and pupils that social networking sites (e.g. Facebook, TikTok, Roblox) are inappropriate and illegal for pupils under the age of 13;
- Encourages staff to regularly check privacy settings of any social networking site that they use at home to ensure privacy;
- For more information on this See SECTION 1 - Education and training for more details.

### **Use of generative AI at St. Stephen's**

At St Stephen's Primary School, we acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the [DfE's guidance](#) on this. In particular:

#### **Student AI platform usage**

- We will talk about the use of these tools with pupils, staff and parents - their practical use as well as their ethical pros and cons. As of April 2025, children in Year 6 learn what AI is and discuss extensively the pros and cons of AI for children and society as a whole. This unit of work is from Kapow.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students - these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- In school, we allow the use of some AI platforms such as Canva AI, which are closely monitored by the specialist computing teacher in class. Currently, the curriculum allows approved AI platforms for children to use and experience, for instance children have produced an AI generated story and image using Canva AI. Additionally, some generative AI 'bundle' platforms are blocked such as Chatgpt and children are unable to access this due to the filtering and monitoring systems setup with LGFL. If and when appropriate these AI platforms can be unblocked on a one-by-one basis for those sites/apps deemed to be acceptable, with limitations according to age or perhaps only for certain lessons or periods of time.

#### **Staff AI platform usage**

Most recently staff have been actively encouraged to use AI to assist with planning and content creation. Tools like ChatGPT or TeachAI can help create age-appropriate, curriculum-aligned lesson plans quickly, as well as generate teaching materials: such as worksheets, quizzes, flashcards, and reading comprehension exercises tailored to student needs. Additionally, AI platforms can also help to produce differentiated content for students at different ability levels, including simplified or enriched versions.

At St Stephen's we hope that using AI can significantly reduce teacher workload and improve work-life balance by automating routine tasks and providing intelligent support in planning, teaching, and assessment.

Teachers can only access AI generated platforms using LGfL WebScreen per user filtering system to access a range of AI platforms.

## **MANAGING EQUIPMENT**

### **Using the school network, Google Workspace, equipment and data safely**

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school is moving towards primarily using Google Workspace as a work space and for cloud storage. Each teacher and Senior Support Staff Member has a chromebook provided by the school for planning and teaching. The school has 3 chromebook trolley's with 30 laptops for classroom use.

*The school reserves the right to examine or delete any files that may be held on its computer system or Google Workspace or to monitor any Internet or email activity on the network.*

### **To ensure the network is used safely, St. Stephens Primary School:**

- Maintains equipment to ensure Health and Safety is followed e.g. equipment installed and checked by approved Suppliers / LA electrical engineers;
- Uses our broadband network for our CCTV system and this has been set-up by approved LGfL partners;
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school computing systems regularly with regard to security.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems e.g. technical support or SIMS Support through LA systems;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role e.g. SEN coordinator - SEN data;
- Similarly on Google Drive not all folders are visible to everyone. Teachers have access to all curriculum and coordinator folders, but folders where sensitive data is stored are only accessible by people who need access to it for their role.

### **For all users**

- Makes clear that no one should log on as another user.
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Request that teachers and pupils switch the computers off at the end of the day and the school automatically remotely switch off all computers at 8 o'clock;
- When a class has used a chromebook trolley all devices should be returned to the trolley and plugged in to charge.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites - except those approved for educational purposes;
- Encourages all users to scan all mobile equipment with anti-virus / spyware before it is connected to the network;

- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their Shibboleth compliant username and password.

#### **For Staff**

- Ensures staff read and sign that they have understood the school's Acceptable Use Form. Following this, they are set-up with Internet and email access and can be given an individual network login username and password;
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Teachers and HLTAs are required to 'sign out' their chromebook for use. They then become responsible for the chromebook and can take it home for work use.
- Makes clear that staff are responsible for ensuring that their chromebook, loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email or Intranet; finance system, personnel system.
- Ensures that access to the school's network resources by staff can only be done on-site or on a school registered device;
- Managed Learning Environment can be accessed online by all staff but is password protected and staff users can only access modules related to their role;

#### **For Pupils**

- Provides pupils with an individual network login username. From Year 1 they are also expected to use a personal password;
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins - these have far less security restrictions and inappropriate use could damage files or the network;

#### **HOW WILL INFRINGEMENTS BE HANDLED?**

*Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management. These guidelines are intended to support teachers when handling these sorts of issues.*

#### **Pupils:**

**Dealt with by class teacher in accordance with behaviour policy e.g.**

- Use of non-educational sites during lessons,
- Use of unauthorised instant messaging / social networking sites.

**Dealt with by class teacher in accordance with behaviour policy and Online Safety Coordinator informed e.g.**

- Continued use of non-educational sites during lessons after being warned,
- Continued unauthorised use of email after being warned,
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups ,
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc,

- Accidentally corrupting or destroying others' data without notifying a member of staff of it,
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

**Dealt with by class teacher in accordance with behaviour policy and Phase Leader/ Online Safety Coordinator / Head Teacher informed and letter sent to parents e.g.**

- Deliberately corrupting or destroying someone's data,
- Violating privacy of others,
- Sending an email or instant message that is regarded as harassment or of a bullying nature (one-off),
- Deliberately trying to access offensive or pornographic material,
- Any purchasing or ordering of items over the Internet,
- Transmission of commercial or advertising material,
- Use of mobile phone (or other new technologies) in school e.g. to send texts to friends

**Dealt with by Head Teacher and parents meeting. Also inform governor pupil disciplinary panel e.g.**

- Continued sending of emails or instant messages regarded as harassment or of a bullying nature after being warned,
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988,
- Bringing the school name into disrepute.

### **Staff:**

#### **Referred to Line Manager**

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.,
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored,
- Not implementing appropriate safeguarding procedures,
- Any behaviour on the internet that compromises the staff members professional standing in the school and community,
- Misuse of first level data security, e.g. wrongful use of passwords,
- Breaching copyright or licence e.g. installing unlicensed software on network.

**Referred to Headteacher / Governors and follow school disciplinary procedures; report to ITASS, report to Police e.g.**

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

#### **Other safeguarding actions:**

- Remove the PC to a secure place to ensure that there is no further access to the PC or chromebook.

- Instigate an audit of all computing equipment by an outside agency, such as the schools computing managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. a computing technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

### **If Child Pornography is found?**

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called: see the free phone number **0808 100 00 40** at:

<http://www.met.police.uk/childpornography/index.htm>

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

[http://www.ceop.gov.uk/reporting\\_abuse.html](http://www.ceop.gov.uk/reporting_abuse.html)

<http://www.iwf.org.uk>

### **How will Staff and Pupils be informed of these procedures?**

- They will be fully explained and included within the school's Online safety / Acceptable Use Policy. All staff will be required to sign the school's Online safety Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate Online safety / acceptable use form;
- The school's Online safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.