St James' Church of England

Junior School

(Voluntary Controlled)

Online Safety Policy

Headteacher:
Rose Boland-Bourne
St James' C of E Junior School
Tower Hamlets Road
Forest Gate
London,   E7 9DA
020 8534 4030

Drawn up by	Lara Dempsey
Date	October 2021
To be reviewed	Autumn 2022

Contents

Introduction

At St James' we believe we have a duty to provide pupils with quality Internet access as part of their learning experience across all curriculum areas and that our provision should reflect the rapid developments in technology. The use of the Internet is an invaluable tool in the development of lifelong learning skills and is central to all aspects of learning, for both adults and children in our school and our wider community. Computing is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults.

We believe that the Internet, if used correctly, will not only raise standards, but will also support teacher's professional work and will enhance the school's management information and business administration systems.

It is important to recognise the constant and fast paced evolution of technology within our society as a whole. Currently the Internet technologies our pupils are using inside and outside of the classroom include, but are not limited to:

- Websites
- Learning platforms and virtual learning environments
- Email and instant messaging
- Chat rooms and social networking
- Blogs
- Podcasts
- Video broadcasting
- Music downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies. At St James', we understand the responsibility to educate our pupils on online-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

All children, whatever their needs, will have access to a range of up to date technologies in school. ICT is a life skill and should not be taught in isolation. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning.

Aims

- Design and deliver a curriculum that builds in the use of technology in order to equip young people with the skills to access lifelong learning and employment

Password Policy

At St James' we:

- Make it clear that staff and pupils must always keep their passwords private, must not share it with others and must not leave it where others can find it
- Make sure all staff have their own unique username and private passwords to access school systems
- Ensure staff are responsible for keeping their passwords private
- Require staff to use strong passwords for accessing our network
- Require staff to change their passwords for school systems regularly

Areas of Risk

The main areas of risk for our school community can be summarized as follows:

Content

- Exposure to inappropriate content, including online pornography, substance abuse, ignoring age ratings in games and television/film content (exposure to violence, inappropriate language etc.)
- Lifestyle websites for example, pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including 'frape'- hacking Facebook profiles) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online)
- Sexting (sending and receiving personally intimate images) also referred to as SGII (self-generated indecent images)

Cyber Crime

- Malware used to steal personal details and credentials
- Copyright (little care or consideration for intellectual property and ownership- such as music and film)
- Spyware used to hack computers

Roles and Responsibilities

This policy applies to all members of St James' CofE Junior School community including staff, pupils, parents/carers, volunteers, visitors and governors alike. It is applicable to all members who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of pupils when they are off school site and empowers members of staff to impose disciplinary penalties to inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data as outlined in the Search and Confiscation guidance issues by the Department for Education. In the case of both acts, action can only be taken over issues covered by the published Behaviour policy.

The school will deal with such incidents within this policy and associated pupil behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place outside of school.

Headteacher and SLT

The Headteacher will:

- Take overall responsibility for online safety provision
- Take overall responsibility for data and data security (SIRO)
- Ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- Ensure all data held on pupils won the learning platform is adequately protected
- Ensure all data held on pupils on the admin machines have appropriate access controls in place
- Ensure all London Grid for Learning services are managed on behalf of the school, including maintaining the LGfL USO database of access accounts

The Headteacher and SLT will:

- Be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as necessary
- Be aware of the procedures to be followed in the event of a serious online safety incident
- Receive regular monitoring reports from the Online Safety Leader
- Ensure there is a system in place to monitor and support staff who carry out internal online safety procedures

Computing/Online Safety Leader

The Computing/Online Safety Leader will:

- Oversee the delivery of the online safety element of the Computing curriculum

- Liaise with the link governor about online safety

Link Governor

The named link governor for Online Safety is Ellen Kemp.

The link governor will:

- Ensure that the school follows all current online safety advice to keep the pupils and staff safe
- Together with the Full Governing Body approve the Online Safety policy and review the effectiveness of the policy
- Ensure regular information about online safety incidents and monitoring reports are received
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Conduct regular reviews with the Online Safety leader including online safety incident logs

Communication

The policy will be communicated to all related personnel in the following ways:

- Online Safety policy to be published to school website and displayed in the staff room
- A copy of this policy will be available in every classroom
- Online Safety policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each academic year
- Acceptable use agreements to be issued to the whole school community, usually on entry to the school and to be resigned when there are major changes
- Acceptable use agreements to be held in pupil and staff personnel files

Handling Complaints

St James' will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, 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. Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- Interview/counselling by teacher/Online Safety Leader/Headteacher/SLT
- Informing parents or carers
- Removal of internet or computer access for a period
- Referral to Local Authority/Police

Our class teachers act as a first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying policy. Complaints related to child protection are dealt with in accordance with the school/LA child protection procedures.

Staff and Governor Training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on online safety issues and the school's online safety education program annually
- Provides, as part of the induction process, all new staff (including those on placement and work experience) with information and guidance on the online safety safeguarding policy and the school's Acceptable Use policy

Email

St James' CofE Junior School:

- Provides all staff and governors with an email account for their professional use (LGfL mail) and makes it clear personal emails should be made through a separate account
- Does not publish personal email addresses of pupils or staff on the school website
- Use anonymous addresses for communication with the wider public (info@st-james.newham.sch.uk)
- Will contact the Police if one of our staff or pupils receives an email that we consider to be disturbing or breaking the law
- Ensure all email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary, the Police
- Knows that spam, phishing and virus attachments can make emails dangerous
- Use a number of LGfL provided technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering
- Use LGfL Webscreen 2 filtering to monitor and protect our Internet access to the World Wide Web

Pupils

Our pupils:

- Use a LGfL pupil email system which is intentionally 'anonymised' for pupil protection
- May only use school/setting provided email accounts for educational purposes
- Are taught about online safety and 'netiquette' of using emails both in school and at home

Staff

Our staff:

- Use LGfL email systems for professional purposes

- May have access to external personal email accounts in school blocked
- Never use email to transfer staff or pupil personal data
- Use a secure file transfer solution or protect the data file with security encryption when transferring data
- Will be encouraged to develop an appropriate work life balance when responding to emails

School Website

The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained. We ensure that:

- Uploading of information is restricted to our website authorisers
- The school website complies with the statutory DfE guidelines for publications
- Most of the material is the school's own work, but where other's work is published or linked, the sources are credited
- The point of contact on the website is the school address, telephone number and we use a general email contact address, info@st-james.newham.sch.uk
- Individual email identities are not published
- Photographs published on the website do not have full names attached and parental permissions have been given
- Pupils' names are not used when saving images in file names or in the tags when publishing to the school website
- Embedded geodata in respect of stored images is not used

Equipment and Digital Content

Personal Mobile Phones and Mobile Devices

- Mobile phones brought into school are entirely at the staff member's, parent's or visitor's own risk
- The school accepts no responsibility for the loss, theft or damage of any phone or mobile device brought into school
- Only students who walk 'home alone' are permitted to bring a mobile phone into school
- Students who bring a mobile phone into school must hand this into the School Office at the beginning of the school day (where it will be securely stored) and collect it at the end of the school day
- Staff members may use their phones during school break times
- All visitors are requested to keep their phones on silent and not use them

- If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf

Staff use of Personal Devices

- Staff are not permitted to use their personal mobile phone or device for contacting children, young people or their families within or outside of the setting in a professional capacity
- Staff will have access to a school phone where contact with pupils, parents or carers is required

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose
- If a member of staff breaches the school policy, then disciplinary action may be taken
- 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 before the number) their own mobile number for confidentiality purposes

Asset Disposal

- Details of all school-owned hardware will be recorded in a hardware inventory
- Details of all school-owned software will be recorded in a software inventory
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed

Equality

Under the Equality Act 2010, we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. As such, we believe that it is in line with the Equality Act 2010, that will not prioritise or disadvantage any pupil and equality will be promoted actively at this school.