ONLINE SAFETY POLICY

1. INTRODUCTION AND OVERVIEW

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

Content

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

Contact

- Grooming.
- Sexual abuse. This can take place online, and technology can be used to facilitate offline abuse (Keeping Children Safe in Education, 2024).
- Sexual Harassment. Including non-consensual sharing of sexual images and videos, sexualised online bullying, unwanted sexual comments and messages, including on social media; sexual exploitation; coercion and threats and upskirting (KCSIE, 2024).
- Cyber-bullying in all forms. This can take place wholly online, or technology may be used to facilitate offline abuse (Keeping Children Safe in Education, 2024).

- Identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords.
- CSE (Child Sexual Exploitation) and CCE (Child Criminal Exploitation)

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Mental Health and well-being (amount of time spent online Internet, impact of cyberbullying or gaming).
- Sexting (sending and receiving of personal intimate content / images).

2. SCOPE

This policy applies to all members of St James the Less RC Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy.

The 2011 Education Act increased these powers with regards to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

St James the Less will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be stored on network location.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in pupil and personnel files.

Handling complaints

The school will take all reasonable precautions to ensure e-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.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Informing parents or carers
- Temporary removal of Internet or computer access for a period
- Referral to LA / Police or other authorities.

Any complaint about staff and student misuse is referred to the Headteacher.

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 child protection procedures.

3. EDUCATION AND CURRICULUM

Pupil e-safety curriculum

St James the Less has a clear, progressive e-safety education programme as part of both the pastoral system and curriculum. It covers a range of skills and behaviours including:

- To STOP and THINK before you CLICK
- To follow the SMART rules for staying safe online
- To develop a range of strategies to evaluate 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 understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.

- To have strategies for dealing with receipt of inappropriate materials.
- To understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To understand how peer on peer abuse can take place online, including sexual harassment (KCSIE, 2024).
- To recognise the impact of technology on mental health and wellbeing.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every pupils will sign and will be displayed throughout the school.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- 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 respect and acknowledge 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;

Staff and Governor training

Our school will:

- provide, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies which are detailed in the staff handbook.
- All staff have general safeguarding training yearly which covers elements of e-safety and INSET provided to all staff centred around E-safety is completed.

Parent awareness and training

Our school will:

- provide advice and guidance for parents, including:
- Use information leaflets, Internet Safety Day, school Splashnews, and the school web site to raise awareness of e-safety.
- Provide suggestions for safe Internet use at home.
- Provide information about national support sites for parents.

4. EXPECTED CONDUCT AND KEY RESPONSIBILITIES

In this school, all users:

- Are responsible for using the school IT systems in accordance with the staff handbook.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

5. MANAGING THE INFRASTRUCTURE

Internet access, security (virus protection) and filtering

Our school:

- has an educational filtered secure broadband connectivity which blocks sites that fall into unsuitable categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- only allows children to access internet sites when adults are present.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of Learning Platforms as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search .
- Informs all users that all computer use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the [system administrator
- 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.
- Provides advice and 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.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to the Website Manager and their support team.
- The school website complies with the statutory DfE guidelines for publications and reviewed on a regular basis
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

- Staff are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the Academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing This school

- Only uses the school supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained for 30 days – system 1, 45 days system 2*), without permission except where disclosed to the Police as part of a criminal investigation.

6.EQUIPMENT AND DIGITAL CONTENT

Personal mobile phones and mobile devices

Staff, Parents and Visitors.

- Mobile phones and personal handheld devices brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- No images, videos or recordings should be taken on mobile phones or personally owned handheld devices within the school or its grounds without the prior consent of the Headteacher **and** the person or people concerned.
- Mobile phones and personally owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets. They should not be used in the presence of children
- Staff may use their phones when not supervising children eg. during break times as long as no children are present. If a staff member is expecting a personal call with no pupils present. Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- 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.
- Staff should not 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 the only calls to be made are with the school office or emergency services.
- Staff are permitted to connect personal devices to the wireless network. All devices connected to this network are logged and filtered under the staff members account.
- Students **must not** bring mobile phones or hand held devices into school. Only special arrangements with the office staff/headteacher will permit a child to bring a phone into school but this will be kept in school office until end of school day.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Reviewed: Autumn 2024