St James CE Primary Academy

Together through faith we will aspire to grow in our understanding of ourselves, in our abilities and in our knowledge of God's wonderful diverse world.

Online Safety Policy

Review Date: September 2026

Introduction

At St James C of E Primary Academy, we understand the responsibility we have as role models to educate our pupils on online safety issues, teaching them 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. We are aware of the risks that our pupils face in relation to these technologies and ensure that they are taught how to react in a variety of situations to minimise risk to themselves or others.

St James C of E Primary Academy has a whole-school approach to the safe use of digital technology and creating this safe learning environment includes three main elements: - a robust provision of network and internet security (provided by Heimdal and Securus) - policies and procedures with clear roles and responsibilities and a comprehensive online safety programme for pupils and staff.

Roles and Responsibilities

Online safety is the responsibility of all staff at St James C of E Primary Academy and even staff who do not use a computer or digital device, need to have an understanding of online safety and its importance.

The DSL and DDSL, Mrs Hewkin and Mr Dobson, have overall responsibility for safeguarding and child protection, including online safety and understanding of the filtering and monitoring systems and processes in place.

The online safety curriculum is the responsibility of the DSL and DDSL and LAC members. All staff are aware that online safety is everyone's responsibility and know that any concerns are to be referred to Mr Dobson or Mrs Hewkin

Staff need to be made aware of any changes to the policy. Staff are updated annually about online safety and its key role in Keeping Children Safe in Education. New staff receive information on the school's acceptable use policy as part of their induction.

All staff receive regular Online Safety updates and a range of Online Safety Briefing emails throughout the academic year. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and must follow school online-safety procedures. All staff should be familiar with the school's policy including:

•safe use of e-mail
•safe use of the Internet, including our filtering and monitoring procedures
•safe use of digital images and digital technologies, such as mobile phones and digital cameras
•publication of pupil information/photographs on school website or school social media sites.
•procedures in the event of misuse of technology by any member of the school community.
•their role in providing online safety education for pupils in line with the online safety long-term plan provided by the computing coordinator.

Managing the school online safety messages

• Promoting online safety messages across the curriculum whenever the internet and/or related technologies are used.

• Delivering online safety lessons regularly throughout the academic year through the PSHE curriculum and Kapow ICT schemes of work.

• The online safety policy will be shared with new staff, including the acceptable use policy as part of their induction.

• Online safety posters will be displayed in all classrooms around the school.

• Internet Safety Day to be promoted every year across the Academy.

• Online safety information for parents to be sent out regularly via the school newsletter.

Curriculum

At St James C of E Primary Academy, we ensure that online safety is taught to children on a regular basis from Reception to Year 6. We have developed a long-term plan for online safety, which is accessible, and progressive, ensuring messages are reinforced each year in an engaging manner and are appropriate for each year group. Each term, every class must be taught a stand-alone online safety lesson in addition to discussions and reminders around the subject whenever digital technology is being used – this is to ensure that online safety messaging happens regularly and is embedded into the curriculum.

As well as teaching online safety via our Relationships and Sex Education, we are continually looking for new ways to promote online safety**.**

• We provide opportunities within a range of curriculum areas to teach about online safety.

• Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise, and formally as part of the curriculum.

• Pupils are aware of the impact of online bullying (child on child) through online safety lessons and PSHE lessons and know how to seek help if these issues affect them.

• Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies.

At St James, we use Kapow for PSHE and ICT, These curriculum schemes have all of the required coverage and applications without the need for external sources.

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material, which makes it both an invaluable resource for education as well as a potential risk to young people.

• Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

• Staff will preview any recommended sites before use.

• Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.

• If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to senior management/DSL. The unsuitable site must be reported to IT support so it can be blocked.

An incident like this should also be logged in the school's safeguarding system (CPOMS).

• Videos should be screened first by staff before being shown to children in lessons.

• Children can search for videos and images for educational purposes but this must be done in a controlled environment.

• Internet filtering is managed by Heimdal and is in place on all devices connected to the school network.

• Children must only access the internet through devices managed by the school network under child login accounts – this is to ensure internet filtering is in place.

• Heimdal filtering monitors key words searched and reports are monitored by the Executive Principal

• Anti-virus management is controlled and monitored by Heimdal

• Internet access can be taken away from children if they are found to be using it inappropriately.

• A class code of conduct is read through, and displayed in every classroom to remind pupils of their responsibilities.

• The DSL completes an Online Safety audit annually and works closely with LAC to ensure it is reflective, fit for purpose and up to date with statutory guidance.

• An Online Safety training log is kept and added to throughout the academic year of training undertaken.

Security and Data Protection

The school and all staff members comply with the Data Protection Act 2018. Personal data will be recorded, processed, transferred and made available according to the act.

• Password security is essential for staff, particularly as they are able to access and use pupil data.

• Staff have secure passwords, which are not shared with anyone.

• All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.

• All staff computers must be locked when the member of staff is away from the machine.

• Staff devices, that have access to school email or the network, must have password, retina or fingerprint protection to ensure sensitive data is safe if the device is lost or misplaced.

• Staff must take care when opening email attachments and be aware of fake emails and scams. Protection against this is in place from Heimdal and Securus.

• Staff should use the 'freeze' or 'blank' option on interactive boards when viewing sensitive information.

• Staff should take extra care when sending emails which include personal information.

Staff Training

All new staff undertake online safety when they are employed. All staff also undertake refresher training every year on online safety and are updated regularly with any new information or advice which is relevant to online safety with regards to the school community. Our online safety training is produced by St Chads, Multi Academy Trust to ensure that all staff receive the most recent and relevant online safety information and messages.

Online safety Complaints/Incidents

As a school, we take all precautions to ensure online safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this.

Complaints should be made to the Executive Principal or Head of School through the appropriate channels. Incidents relating to online safety could involve staff, volunteers, visitors or children and in some cases may take place beyond school.

Incidents may be in relation to unsuitable use or unsuitable material, or in extreme cases, illegal use or material. In either case, it is the responsibility of the staff member who witnessed the incident to follow it up in line with the school's behaviour policy. This may require them to inform a Designated Safeguard Lead (DSL) or deal with incident themselves, depending on the seriousness of what happened. In any case, it must be logged in our behaviour and safeguarding software (CPOMS).

Any safeguarding issues, related to online safety, must be reported to a Designated Safeguard Lead (DSL) and logged on our safeguarding software (CPOMS).

When an incident has occurred and been passed on to a DSL or member of the senior management team, it is then their responsibility to take appropriate action.

Online safety incidents involving children will follow the behaviour policy where necessary and appropriate.

Social Media and Website

At St James C of E Primary Academy, we use Facebook, the school website and our school newsletter to promote children's achievements and work and to strengthen the link between home and school. Children's photos and work will only be posted on school social media sites if permission is granted from parents or carers. Permission is given or denied by the child's parent or carer when they are admitted to the school. If this decision is changed, it is the parent or carers' responsibility to contact the school.

Names of children should not be posted alongside their photo in any public domain. Staff are advised to ensure that their personal social media accounts are private and to use their social media accounts responsibly.

Online safety Outside of School

Children have access to many forms of digital technology outside of school. The safe use of these technologies outside of school is the ultimate responsibility of the child's parents or carer(s).

However, at St James, our whole school approach to online safety extends to the parents. We do, and will, give any information or advice to parents and carers that is requested regarding online safety. This includes, but is not restricted to, annual Online Safety workshops, regular information sharing and updates to parents, updated information on the school website.

In addition to this, information on setting up parental controls, advice on age ratings and general advice about staying safe online are available on our Academy website.

The CEOP report button is also available on the Safeguarding page on our website.

Children are encouraged to report incidents that happen outside of school to members of staff so that advice can be given and so action can be taken when appropriate.

Mobile and Smart Technology

We understand that both adults and children make use of mobile and smart technology more than ever. This comes with risks in a school environment and at St James C of E, we have put in place rules to ensure that risk is minimised.

Staff Devices

Staff are allowed to have personal devices in school such as a mobile phone or tablet. These are to be switched off in the classroom and can be used during break times in the staffroom or outside of the academy building.

Staff are not permitted to take videos of photos of children using their personal devices.

Staff should not make calls or send messages from their phones in any area of the school where they can be heard by the children. If a member of staff needs to make a call or send a message, it should be done in an area where no children are present (for example, the staffroom/staff office or room which is empty with the door closed)

Pupil Devices from home

We are aware that some of our Year 6 pupils, who walk home after school, will bring their mobile phone into the academy.

• Children must not use their phone for any purpose once on school grounds and they will switch it off at the school gate.

• Children must hand their phone in to the office as soon as they walk into the building.

• If a child does not follow the above rules, their phone will be confiscated and their parent or guardian will be called. In these instances, the phone will be kept in school until a parent or guardian collects it.

• If any of these rules are broken repeatedly, the school has the right to ban any child from bringing their phone and give consequences linked to the school's behaviour policy.

• If a child's phone gets damaged in any way, or lost on school grounds, it is not the school's responsibility.

Smart Watches – Staff and adults in school

Staff are permitted to wear and use smart watches in school. As with mobile phones or tablets, staff must not use them for personal activities during lesson times, but they are free to do so during their free time in an appropriate area of the school. Staff can use smart watches for educational purposes during lesson times (for example, as timers or stopwatches).

Smart Watches – Pupils

Pupils are not permitted to wear smart watches in school. Pupils who come to school wearing a smart watch will be asked to remove it and hand it in to a member of staff who will return it at the end of the day. Parents will be informed and asked that it is not brought in again. If a pupil persists to wear a smart watch to school after the first time, then action will be taken in line with the school's behaviour policy. Children are permitted to wear analogue or digital watches that do not have connectivity to the internet or other mobile devices.

Online-Bullying

At St James C of E we take online-bullying very seriously. All incidents will be logged in CPOMs and the Executive Principal and Head of School will be made aware. An incident of online-bullying will be dealt with in accordance with the procedures in the school's Anti-Bullying Policy. Keeping Children Safe in Education 2023, states that Child on Child abuse can happen online and between children of different ages.

Harmful online challenges and online hoaxes

If we are aware that a harmful online challenge or hoax is in circulation amongst children and young people, the Executive Principal and Head of School will undertake a case-by-case assessment to establish the scale and nature of the possible risk to children and young people at St James C of E. This will include consideration whether the risk is a national one or if it is localised to our area, or our school. If necessary, a measured response that avoids causing panic or confusion will be made by the school to inform parents about the harmful online challenge or online hoax. In some cases, it will not be appropriate to share details about the concern; this will be decided after an assessment of the risk and nature or the challenge or hoax. It may also be necessary in certain cases to share information about a challenge or hoax with children, but this will always be done after careful consideration with an aim to not distress or scare them or inadvertently lead them to the content.

As part of our online safety programme at St James C of E, we teach children methods to help reduce the impact of harmful online challenges and online hoaxes and fake news, such as fact checking and how to report anything that concerns them online. By modelling and teaching 'good online behaviour', we aim to reduce the risk that harmful online challenges and online hoaxes/fake news pose to our pupils.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include;

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded ;o denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and, making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

If a member of staff suspects a member of the school community is involved in cybercrime, they will report it to the DSL or DDSL who will deal with the incident – the designated safeguarding lead or DDSL may need to seek further advice from agencies such as the police or Family Connect. In addition to this, if there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring the child into the 'Cyber Choices' programme.

Review

This policy will be reviewed every year but will be updated before that time, if necessary. Any changes will be verified with the Executive Principal and/or Head of School and LAC.