Online Safety Policy

Adopted by the Governing Body: May 2016	
Date Last Reviewed: December 2023	**Next Review Date:** September 2025
Signed: *L Constable* (Headteacher)	**Signed:** (Chair of AGC)

Introduction

Online safety encompasses Internet technologies and electronic communications, including tablets and mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The school's Online Safety policy will operate in conjunction with other school policies including the:

- Behaviour policy
- Anti-bullying policy
- Child protection and Safeguarding policy
- Curriculum policies
- Data protection policy
- Security policy

Online safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of our Online Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband with appropriate filters wherever children have access to the internet
- National Education Network standards and specifications.

St James' Online Safety Policy

Our Online Safety Policy has been written by the school, building on the Warwickshire County Council Online Safety Policy and government guidance. It has been agreed with teachers and approved by members of the AGC.

The Online Safety Co-ordinator is Becki Estano, IT and Computing Leader

The Child Protection Coordinator is the Headteacher, Laura Constable

The member of the AGC with responsibility for Safeguarding is Sara Wisniewski.

The Online Safety policy and its implementation will be reviewed every two years, or earlier if Local Authority guidance is updated.

Roles and Responsibilities

Members of the AGC

The role of the Safegaurding governor, overseeing online safety too:

- Meeting with the Online safety co-ordinator once a term.
- Regular monitoring of any online safety incident log.
- Regular monitoring of filtering
- Reporting back at AGC meetings
- Attending suitable training to carry out this role

Headteacher and Senior Leadership

The role of the Headteacher / Senior Leadership will include:

- Ensuring the safety (including online safety) of members of the school community
- Understanding and being able to follow the procedures in the event of a serious online safety allegation being made against a member of staff
- Ensuring that all teachers and teaching assistants receive suitable training to enable them to carry out their online safety roles and to train other colleagues.
- Ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role

Online Safety Co-ordinator

The role of the Online Safety Co-ordinator will include:

- Referring safeguarding /Child protection concerns to the Designated Safeguarding Lead without delay.
- Leading the online safety committee
- Taking day to day responsibility for online safety issues as well as reviewing the school online safety policies
- Ensuring all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff
- Liaising with the Local Authority/MAT ICT advisors
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments. This log will form part of the serious incident log.
- Meeting regularly with the Safeguarding Governor.
- Reporting regularly to the Senior Leadership Team.

Technical Staff

The role of the school's technical support (managed by SoftEgg) will include:

- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the school meets required online safety technical requirements and any Local Authority / other relevant body Online Safety Policy / Guidance that may apply.
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Making sure they have an up to date awareness of online safety matters and of the current online safety policy and practices
- Ensuring that they have read, understood and signed the Staff Acceptable Use Policy
- Ensuring that they report any suspected misuse or problem to the Head of School / Online safety Co-ordinator for investigation / action / sanction

Teaching and Support Staff

The role of the teaching and support staff will include:

- Having an up to date awareness of online safety matters and of the current school online safety policy and practices
- Ensuring they have read, understood and signed the Staff Acceptable Use Policy
- Reporting any suspected misuse or problem to the Headteacher/ Online Safety Coordinator for investigation / action / sanction
- Ensuring that all digital communications with students / pupils / parents / carers is on a professional level and only carried out using official school systems
- Ensuring online safety issues are embedded in all aspects of the curriculum and other activities
- Ensuring pupils understand and follow the Online Safety and Acceptable Use policies
- Ensuring pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Monitoring the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 online safety practice when using digital technologies out of school and realise that the school's Online Safety policy covers their actions out of school, if related to their membership of the school
- Will adhere to the KS1 and KS2 Online Safety Rules.

Teaching and Learning

Staff and members of the AGC at St James recognise that:

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- When the internet is required for home learning pupils will have their own login which will be required
- When virtual meetings are needed, we will use a recognised platform in which an invitation will be sent to individuals and a waiting room will be used to ensure safety of use.

As part of the School's Computing Curriculum, pupils will be taught:

- How to use the Internet effectively to locate, retrieve and evaluate materials in order to enhance and extend their learning, using search tools appropriate to their age
- What Internet use is acceptable and what is not and given clear objectives for Internet use.
- That they must comply with the law when copying and subsequently using Internet-derived materials. This will include acknowledging the source of information used and respecting copyright when using Internet material in their own work.

The Management of Information Systems

- The school Internet access is provided by
- The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

The Management of E-Mails

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- ClassDojo will be used for group communication with parents.
- Staff will only use official school provided email accounts and ClassDojo to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.
- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

The Management of Published Images

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers to publish images/videos of pupils electronically will be updated annually.
- Pupils' work can only be published with their permission or their parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

The Management of Social Network Sites

- The school will control access to social media and social networking sites.
- Pupils will be taught never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

The Management of Filtering Systems

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with the MAT ICT provider and/or WCC and/or the Schools' Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Coordinator, who will then record the incident and escalate the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as Warwickshire Police
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

The Management of Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use and Mobile Phone Policy.

The Protection of Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the GDPR regulations.
- Personal data for staff and pupils will be held on the admin server. Access to this data will be limited to members of the SLT and approved admin staff.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff and members of the AGC will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources or personal equipment on site.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy. Internet access by pupils
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school, MAT or WCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Warwickshire Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Responding to and Reporting Incidents of Concern

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyber bullying, illegal content etc.).
- The Online Safety Coordinator will record all reported incidents and actions taken in the school online safety incident log and other in any relevant areas e.g. Bullying or Child Protection log.
- The Designated Safeguarding Lead will be informed of any online safety incidents involving child protection concerns, which will then be escalated appropriately.
- The school will manage online safety incidents in accordance with the school Behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place, or the school is unsure how to proceed with any incidents of concern, then the school will contact the MAT Central Team and the Local Authority's Online Safety officer (Jane Key), escalating the concern to the Police if necessary.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Local Authority's Online Safety Officer (Jane Key) and the MAT Central Team to communicate to other schools in Warwickshire and the MAT.

Online Safety Complaints

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- All online safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure which is available on the school's website.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with Warwickshire Police (Children, Youth and Schools section) and/or Children's Safeguarding Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Cyber Bullying

Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Please refer to the school's Behaviour policy and Anti-bullying policy.

- All incidents of cyber bullying reported to the school will be investigated in line with the Antibullying policy and will be recorded on a bullying log sheet.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in cyber bullying may include:

- The alleged perpetrator will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the alleged perpetrator refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools Anti- bullying, Behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected. The use of mobile phones and other personal devices for staff and pupils
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- For further details please refer to the school's Mobile Phone Policy for staff and pupils Communicating the online safety policy to pupils
- All users will be informed that network and Internet use will be monitored.
- An online safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access in computing lessons and across other curriculum subjects.
- An online safety module will be included in the Computing curriculum, covering both safe school and home use.
- Online safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Particular attention to online safety education will be given where pupils are considered to be vulnerable.

Communicating the Online Safety Policy to Staff

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils. Staff will be expected to read and comply with the Staff Information Systems Code of Conduct .
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

Communicating the Online Safety Policy to Parents

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus and on the school website.

• A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting online safety at other attended events e.g. parent evenings and sports days.
• Parents will be requested to sign an Online Safety/Internet agreement as part of the Home School Agreement.
• Parents will be asked to read the school's online safety rules and discuss the Acceptable Use Policy for pupils, signing these documents with their children.
• Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents via the school website. Community use of the internet
• All use of the school's Internet connection by community or other organisations shall be in accordance with the school's online safety policy.

E-Safety References

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
www.thinkuknow.co.uk www.internetmatters.org
Childline: www.childline.org.uk
Childnet: www.childnet.com
Cybermentors: www.cybermentors.org.uk
Digizen: www.digizen.org.uk

E-Safety Contacts

Warwickshire Online Safety Officer: Jane Key key.j2@welearn365.com
Phone: 01926 414100 (ICTDS service desk)

Children's Social Care Initial contact is to be made through the Multi-Agency Safeguarding Hub (MASH)
Phone: 01926 414144 Mon-Thu: 8.30am – 5:30 pm Fri 8:30am – 5:00 pm
Outside these hours, the emergency number is: 01926 886921

Warwickshire Police: In an emergency (a life is in danger or a crime in progress) dial 999 or 112
For other non- urgent enquiries contact Warwickshire Police via the non-emergency line on 101.