St. George's Junior School
E-safety Policy

Empower Multi-Academy Trust

ST GEORGE'S JUNIOR SCHOOL SHREWSBURY

June 2025

E-safety Policy

St. George's Junior School is committed to safeguarding and promoting the welfare of all children. We expect all staff, parents and volunteers to share this commitment.

- The e-safety leader in St George's Junior school is Charlotte Worley, also DSL. Jake Mansel is also a named point of contact for any online safety needs.
- Charlotte Worley is accredited as a CEOP ambassador and disseminates training to stakeholders in this role.
- This policy has been written by the schools and agreed by all staff and governors.
- This policy applies to all members of our school community.
- This policy is backed up by an online safety risk assessment and monitoring procedures.

1. The importance of e-safety

Internet use is a necessary tool to aid learning and development in the 21st century. Pupils use the internet widely outside of school, including the use of apps, games, websites and FaceTime and need to learn how to navigate these applications safely and respectfully. As a result, St George's Junior School builds on these experiences and ensures children are equipped with the knowledge they need to protect themselves whilst online.

"The internet is a huge part of our lives. Whichever way you look at it, it has grown to influence every nook and cranny of our society and the way that our "children engage with information". Our parents used to warn us about 'stranger danger', now we teach our children the same lessons, but for a huge, ever-evolving environment. Our young people enjoy spending time on the internet and interacting with their friends and peers online, but this also means that cyberbullying and other online problems can be particularly hurtful."

https://www.educare.co.uk/news/safer-internet-day-2016:-the-importance-of-teaching-your-child-about-e-safety

The use of information and communication technology (ICT); is a vital part of the everyday functioning of and life in school. We also recognise the important role ICT plays in the lives of our children and their families.

Whilst there are many benefits and strengths in using ICT; there are also several risks to children's welfare and safety in school when using internet enabled technology; which are summarised in the following categories:

- **content:** being exposed to illegal, inappropriate, or harmful content.
- **contact:** being subjected to harmful online interaction with other users.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm to children or others.
- **commerce:** illegal, inappropriate, or harmful online commercial activities that can compromise the health and wellbeing or security of children or others.

2. Organisation and provision

We adopt a whole school approach to online safety which aims to safeguard and educate our children and their families, staff, visitors and our school in our use and management of ICT (including the use of camera enabled; mobile and personal devices and the ICT systems we have in place).

All staff and governors have/or are due to receive training on the expectations, applicable roles and responsibilities in relation to filtering and monitoring. This is delivered by the E-Safety Lead.

Staff in each class have access to a desktop computer, a home use enabled laptop and pupil laptops.

Children have access to ipads, LBQ tablets and laptops which have a variety of apps downloaded onto them to support the curriculum. Using these devices, the children have access to the internet and internet-based applications including our Seesaw learning platform. The internet on these devices is filtered by Roartech according to the age group we teach. Children do not use the devices unsupervised.

These resources are essential to the delivery of our curriculum.

3. Filtering and Monitoring of the internet at St George's Junior School

Alongside, Roartech and Lightspeed Systems, we review our online safety arrangements annually to ensure that we meet the Keeping Children Safe in Education and Safeguarding children and protecting professionals in early years settings: online safety considerations online safety standards (including the digital standards for filtering and monitoring and cyber security). Any risks arising from our reviews are clearly recorded as part of our school evaluation and improvement action planning processes. These are reported to and overseen by our Governing Body.

All Staff, senior leaders and Governors are appropriately trained to enable them to ensure effective online safety arrangements. We will respond to online safety incidents which indicate safeguarding concerns in line with our policies.

The E-Safety Leads have completed a 360 safe review of our online safety and an action plan proceeds this to ensure e-safety is of highest priority. A risk assessment also compliments the provision in place to ensure online safety is of highest importance.

Annual monitoring of our filtering processes take place with the E-Safety Leads, Headteacher, Roartech and the link governor. We use The South West Grid for Learning's (SWGfL) testing tool to check that our filtering system is blocking access to:

- illegal child sexual abuse material
- unlawful terrorist content
- adult content

The outcomes of these tests are recorded and filed with the Headteacher using the SWGfL checklist.

4. Assessing risk

The school will take all necessary precautions to prevent access to inappropriate material. However, due to the international scale of the internet it is not possible to guarantee that unsuitable material

will never appear on a school computer. The school will continue to use Roartech and Lightspeed Systems support to filter out inappropriate material and ensure IT equipment is as safe as can be, as per the filtering and monitoring statement above. The school will annually audit this policy and procedures to ensure it is still suitable and effective.

5. Teaching and learning

As a school, we celebrate safer internet day during February of each year. This is a national celebration and helps to raise the profile of e-safety.

Staff have detailed e-safety planning to follow with age-appropriate resources to share with children.

We use the education for a connected world document and project evolve platform to ensure children are educated in all areas of online safety.

All children and staff from both schools sign an Acceptable Use Policy (AUP).

6. Internet use

- During teacher led lessons, children will access safe materials via the internet in school.
- Staff will review all content before pupil's access websites or online applications.
- Pupils are taught to use child friendly search engines and websites e.g. national geographic for kids.
- Pupils are taught that passwords and QR log in codes are private and not to be shared.
- As per the AUP, pupils are taught, via e-safety lessons, to report any hurtful or inappropriate content to a trusted adult.
- Through our e-safety lessons, pupils are taught how to behave whilst using the internet and what is deemed as acceptable and unacceptable behaviour.
- As part of teacher led lessons, children are given a degree of freedom with searches and taught what to do if they come across any content that they are unsure of.

7. Parent support

Through monthly e-safety newsletters uploaded to our website, parents are given e-safety tips and support. Parents are also signposted to a range of websites to help support e-safety at home through a booklet. The E-Safety Lead also shares a presentation to parents to support e-safety at home and at school.

8. Reporting procedures

If access has been gained to inappropriate material, staff will report this by making a log on CPOMS. This will then be followed up by a member of SLT and DSL. If the incident relates to child protection, then the child protection policy procedures will be followed.

Any school cyber security incidents will be reported to Action Fraud (National Fraud and Cyber Crime Reporting Centre) and, if there is a data breach this will be reported in line with our Data Protection Processes to the Information Commissioners Office.

9. E-safety complaints (staff use)

- Complaints of internet misuse will be handled by a senior member of staff.
- Any complaint about staff misuse will be referred to the Headteacher and recorded following policy and procedure.
- Complaints relating to child protection will be dealt with according to our child protection policy.

10. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

11. The use of Artificial Intelligence Tools

St George's Junior school hold an Artificial Intelligence Policy that discusses this.

Key Stage 2 Acceptable Use Rules and Responsibilities

ST GEORGE'S JUNIOR SCHOOL SHREWSBURY

So that I am safe I agree that I will:

1. I will ask permission before using any ICT equipment (e.g. computers, digital cameras, etc), and only use it when a teacher or another adult is with me
2. I will only use the school's computers for schoolwork
3. I will only delete my own files, and I will not look at other people's files without their permission
4. I will use the usernames and passwords provided by the school to access programmes as instructed by staff
5. I will not bring software or USB memory sticks into school without permission
6. I will ask permission before using the Internet, and only use it when a staff member is present
7. I will only visit websites that I am asked to by school staff, or that have been that have been deemed appropriate by staff
8. I will not use Google image search without being asked to do so by a school staff member
9. I will not download anything (files, images etc) from the Internet unless given permission
10. I will only use an approved email account provided for me by the school to send email as part of my learning. I will not use personal email accounts (e.g. Hotmail) at school
11. The messages I send or information I upload as part of my school work will always be polite
12. I will not give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family or my friends, unless my teacher has given permission
13. If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it, but I will immediately tell a school staff member
14. I will follow the **SMART** rules and use information from the **Kidsmart** and **think you know** websites to help me understand how to keep safe when using ICT
15. I understand that the school may check my computer files, e-mail and the Internet sites I visit, to help keep me safe
16. I understand that if I deliberately break these rules my parents and the Headteacher will be informed
17. I am aware of the CEOP website and know how to report something at: www.ceop.police.uk

CEOP REPORT ceop.police.uk

Acceptable Use Policy for staff and visitors to St George's Junior School

This agreement is designed to ensure all staff and visitors are aware of their professional responsibilities when using any form of ICT.

- I will only use the school email, internet and any related technologies for professional purposes.
- I will comply with the school's ICT system and not disclose any passwords provided to me by the school.
- I will not browse, download, upload or distribute any material that could be deemed as offensive, illegal or discriminatory.
- I will ensure any electronic communications with pupils and their families are compatible with my professional role.
- I will only use my approved school email address for school business.
- Any sensitive and confidential data I produce will be stored on a password secured laptop or password protected storage device.
- Images of pupils will only be taken on school owned devices and will not be taken outside of school without the permission of the parent/carer.
- I will comply with the filtering and monitoring procedures of the school and record any online safety concerns to the DSL/DDSL using CPOMS.
- I understand that my social media presence can be researched and any detrimental remarks about the school will be acted upon.
- I will only use my mobile phone or personal device in designated areas when pupils are on the school site.

I agree to follow and adhere to this e-safety guidance and will support the school's approach to online safety.

Signed …… Date …….

Be smart on the internet

Childnet International
www.childnet.com



S SAFE Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Information you find on the internet may not be true, or someone online may be lying about who they are.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

THINK U KNOW

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

