Russell Street School

eSafety Policy

RSS children are **STARS** – Safe, Together, Achieve, Resilient, Special.

Reviewed on:	December 25
Next Review:	Annually
Staff Responsibility:	DSL/DDSLs eSafety Officer Headteacher

2.1 Introduction

The e-Safety Policy relates to other policies including those for AUP, Behaviour, GDPR and for child protection.

- The school e-Safety Coordinator is Mrs Jayne Van Rooyen

2.2 Teaching and learning

2.2.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. It will block harmful and inappropriate content without unreasonably impacting teaching and learning.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

- Pupils will be shown how to publish and present information to a wider audience.

2.2.4 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught how to recognise inappropriate material and report it to a responsible adult.

2.3 Managing Internet Access

2.3.1 Information system security

- School IT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed ITSS Support and E2BN.

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

2.3.3 Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

2.3.4 Publishing pupil's images and work

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused.

- Pupils names will not be used anywhere on a school Website or other on-line space, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil image file names will not refer to the pupil by name.

2.3.5 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.3.6 Managing filtering and monitoring

- The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre.

- There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly. Devices that are provided by the school have school-based filtering applied irrespective of their location.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing video conferencing & webcam use

- Video conferencing should use the educational broadband network to ensure quality of service and security.

- Pupils must ask permission from the supervising teacher before making or answering a video conference call.

- Video conferencing and webcam use will be appropriately supervised for the pupils' age.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

- The use of A.I (Artificial Intelligence). The school acknowledges the potential benefits of the use of AI in an educational context. Staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.

- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school. A DPIA must be completed before any pupil information is shared with a third party.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection legislation.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' for our school.

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- Across the school, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

- Parents will be asked to sign an electronic consent form.

2.4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access.

- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)

2.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

- A programme of training in e-Safety will be developed and embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

2.5.2 Staff and the e-Safety policy

- This policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school.

- Staff must be aware that network and Internet traffic can be monitored and traced to the individual user.

2.5.3 Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.