Russell Street School

Reviewed on:	February 2023
Reviewed:	Annually
Staff Responsibility:	e-Safety Officer, DSL/DDSLs, Headteacher

ICT Acceptable Use Policy

Applies to:	All staff and pupils
Monitoring and reporting.	• System is monitored on a regular basis by the e-Safety Lead • Infringements are reported to the E- Safety Lead • The e-Safety Lead is Mrs Van Rooyen.
Reporting Accidental Access.	• Pupils report to responsible adult who then notifies a member of the senior leadership team.
Reporting Deliberate Abuse or Misuse.	• Pupils report any misuse to responsible adult who then notifies a member of the senior leadership team. • Internet provision is protected by E2BN
Sanctions for misuse.	• Temporary or permanent withdrawal of access to system. • Suspension or exclusion. • Disciplinary or legal repercussions.
Anti Virus and Anti Spam.	• System monitored by E2BN / MKSP ITSS. • ICT technicians to update software when appropriate.
E-mail.	• Staff and pupil e-mail addresses are not to be published. • School e-mail to be used for school business only. • No racist, abusive or bullying language to be used. • Pupils check with a responsible adult before opening any suspicious mail.
Internet usage.	• Pupils are not permitted to download images or sounds without first checking with a responsible adult. • Pupils may only access sites approved by their responsible adult who will also monitor the content of the sites used. • Accidental access to be reported to a responsible adult and then to a member of the senior leadership team. • Websites used in class must be firstly checked by the responsible adult for appropriate content. • Staff are not permitted to store personal images or music on their school laptops. • You Tube is ONLY to be accessed by adults.
Copyright and plagiarism.	• No direct or indirect copying of material without acknowledging the source.
Video conferencing.	• Only to be done with a responsible adult present.

Mobile devices.	• Images of pupils must only be stored on the shared folder and removed when those children have left the school. • Documents that contain pupil addresses and dates of birth must not be store on personal devices. • Personal mobile devices must not be used in school. They must not be used for school business without the headteachers permission. • Any personal devices that are able to take photographs must not be worn in school.
Passwords.	• Passwords that are at least 8 characters long containing letters and numbers are used to access school computers and laptops. Staff are reminded to change their passwords at regular intervals. • Passwords are not shared with other members of staff or pupils. • Laptops are encrypted. • iPads have a six figure passcode.
Security.	• Laptops and other ICT resources need to be locked away when not in use. • ICT resources should not be left in vehicles. • The school business manager needs to be made aware of any change to an item's location.
Safeguarding of children.	• Staff must read and be aware of the school e-Safety policy. • At school performances parents must be reminded not to publish photos or videos online. • Photos of pupils must be stored on the school's server and not on individual devices.
Definition of unacceptable use	The below is considered unacceptable use. Any breach of this policy may result in disciplinary or behaviour proceedings. Unacceptable use of the school's ICT facilities includes: • Using the school's ICT facilities to breach intellectual property rights of copyright. • Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination. • Breaching the school's policies or procedures. • Any illegal conduct, or statements which are deemed to be advocating illegal activity. • Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate. • Activity which defames or disparages the school, or risks bringing the school into disrepute. • Sharing confidential information about the school, its pupils, or other members of the school community. • Connecting any device to the school's ICT network without approval from authorised personnel. • Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.

	• Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel • Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities • Causing intentional damage to ICT facilities • Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel • Causing a data breach by accessing, modifying or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation. • Using inappropriate or offensive language • Promoting a private business, unless that business is directly related to the school. • Using websites or mechanisms to bypass the school's filtering mechanisms. • This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.