Mission Statement
"A Caring Christian Family Where We Grow Together"

E-SAFETY PROCEDURE

Effective Date: 01/04/2017 **Review Date:** Sept 2022 Biennial

Review Date	Signed Head Teacher	Signed Director RCSAT
09/09/2018		
30/09/2020		

Persons Responsible for Policy:	Executive Headteacher RCSAT
Approval Date	01/04/2017
Signed:	Director RCSAT
Signed:	Executive Headteacher RCSAT

1. Introduction

1.1. E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology.

1.2. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

1.3. The school's e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Curriculum, Data Protection and Security.

2. Why is Internet Use Important?

2.1. The purpose of Internet use in RCSAT schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

2.2. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction.

2.3. Access to the Internet is an entitlement for pupils who show a responsible and mature approach to its use. RCSAT schools have a duty to provide pupils with quality Internet access.

2.4. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

3. Internet Use Benefitting Education

3.1. Benefits of using the Internet in education include:

3.1.1. access to world-wide educational resources including museums and art galleries;

3.1.2. inclusion in the National Education Network which connects all UK schools;

3.1.3. educational and cultural exchanges between pupils world-wide;

3.1.4. access to experts in many fields for pupils and staff;

3.1.5. professional development for staff through access to national developments,educational materials and effective curriculum practice;

3.1.6. collaboration across support services and professional associations;

3.1.7. improved access to technical support including remote management of networks and automatic system updates;

3.1.8. exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

3.2. <u>Internet use enhances learning through</u>:

3.2.1. The school Internet access shall be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

3.2.2. Pupils shall be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

3.2.3. Internet access shall be planned to enrich and extend learning activities.

3.2.4. Staff shall guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.

3.2.5. Pupils shall be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

3.3. <u>Authorised Internet Access</u>.

3.3.1. The school shall maintain a current record of all staff and pupils who are granted Internet access.

3.3.2. All staff shall read and sign the 'Acceptable Use Agreement' before using any school resource.

3.3.3. Parents shall be informed that pupils will be provided with supervised Internet access.

3.3.4. Parents shall be asked to sign and return a consent form for pupil access.

3.4. <u>Information System Security/Filtering</u>.

3.4.1. The school will work in partnership with the Local Authority, Becta and the Internet Service Provider to ensure filtering systems are as effective as possible.
3.4.2. School IT systems capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly.
3.4.3. Security strategies will be regularly discussed with the Local Authority. The technician shall update anti-virus software regularly.
3.4.4. Securus monitoring software is used and shall be monitored daily by Deputy Designated safeguarding lead. This monitors access to website and identifies key words and phrases deemed to be inappropriate.
3.4.5. Access to the internet, either through the network or via Wi-Fi is filtered through the Cheshire East Proxy Server. Both these systems filter materials to ensure all users are safe from inappropriate material including terrorist and extremist as required by the Prevent Duty. Inappropriate website shall be blocked through this system.
3.4.6. Pupils and parents shall be aware of the school rules for responsible use of computing resources and be aware of the consequence of any misuse.
3.4.7. The agreed rules for safe and responsible use shall be displayed in all classroom and computing areas.

4. **World Wide Web**

4.1. If staff or pupils discover unsuitable sites, the URL (address), time, content shall be reported to the Local Authority helpdesk via the Pastoral Manager**,** or in their absence, a member of SLT.
4.2. RCSAT schools shall ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
4.3. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

5. **E-mail**

5.1. Pupils may only use approved e-mail accounts on the school system.
5.2. Pupils shall tell a teacher as soon as possible if they receive offensive e-mail.
5.3. Pupils shall not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
5.4. Only whole class or group e-mail addresses shall be used in school.
5.5. Access in school to external personal e-mail accounts may be blocked.
5.6. E-mail sent to external organisations shall be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
5.7. The forwarding of chain letters/chain emails is not permitted.

6. **Social Networking**

6.1. School shall block/filter access to social networking sites is blocked and filtered where possible in line with Local Authority.
6.2. Pupils shall be advised never to give out personal details of any kind which may identify them or their location.
6.3. Pupils shall be advised not to place personal photos on any social network space.
6.4. Pupils shall be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
6.5. Pupils shall be encouraged to invite known friends only and to deny access to others.

7. **Managing Emerging Technologies**

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

8. **Published Content and the School Web Site**

8.1. The contact details on the Web site shall be the school address, e-mail and telephone number.
8.2. Staff or pupils personal information shall not be published.
8.3. The Principal/Headteacher or nominee shall take overall editorial responsibility and ensure that content is accurate and appropriate.

9. **Publishing Images & Work**

9.1. Photographs that include pupils shall be selected carefully and shall not enable individual pupils to be clearly identified.
9.2. Pupils' full names shall not be used anywhere on the Web site or Blog, particularly in association with photographs. **"**Photograph/no name" or "Name/no photograph".
9.3. Written permission from parents or carers shall be obtained before photographs of pupils are published on the school Web site.

10. **Protecting Personal Data**

10.1. Personal data shall be recorded, processed, transferred and made available according to the Data Protection Act 1998.

11. **Assessing Risks**

11.1. RCSAT schools shall take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Cheshire East Council can accept liability for the material accessed, or any consequences of Internet access.
11.2. The school shall audit regularly to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

12. **Handling E-Safety Complaints**

12.1. A senior member of staff shall deal with complaints of Internet misuse.
12.2. Any complaint about staff misuse shall be referred to the Principal.
12.3. Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
12.4. Pupils and parents shall be informed of the complaints procedure.

13. **Communication of Procedure**

13.1. <u>Pupils</u>
13.1.1. Rules for Internet access shall be posted in all networked classrooms.
13.1.2. Pupils shall be informed that Internet use will be monitored.
13.2. <u>Staff</u>
13.2.1. All staff shall be given the School e-Safety Policy and its importance explained.
13.2.2. Staff shall be made aware that Internet traffic can be monitored and traced to the individual user.
13.2.3. Discretion and professional conduct is essential.
13.3. <u>Parents</u>
13.3.1. Parents' attention will be drawn to the School e-Safety Policy and Procedure.

Appendix 1
Responsibilities

Area of Responsibility	**Responsible Person's**
Overall responsibility	Executive Headteacher
Co-ordinator in School	Principal Bunbury Principal St Oswald's Principal Warmingham
Pastoral Manager	Katherine Charlesworth
Governor	RCSAT Governor
Routine E-Safety checks	Pastoral Manager
Daily checks	IT Technician

Appendix 2

E Safety Non-Negotiables

- All staff personal equipment from home – phones, Ipads, laptops, tablet to have a password/passcode set.
- All KS2 and Y2 children must use their own log on and must log off after use. Y1 to be taught during Y1 how to do this. Keep passwords in a safe place when not being used.
- All machines to be logged off when not in use including staff and office computers particularly at lunchtimes. Remind children to log off after use.
- E-safety rules displayed. Rules read weekly (minimum requirement)
- No computers or Ipads to be used during inside/wet playtimes.
- Golden/Reward Time – no use of games websites. Has to be a directed activity discussed with teacher.

Appendix 3

Website Non –Negotiables

- Office Staff – update the calendar with trips, assemblies, events, PTA, general school events e.g. parents evening dates
- Policies and Website layout – Resources RCSAT
- News Page – for specific events e.g. fundraising activities
- Nic Badger - Sport's Page Bunbury
  Alex Goodwin - Sport's Page St Oswald's
  Kate Appleby - Sport's Page Warmingham
- Teachers Class Page – update regularly with general info, topic overview, photos
- Teacher News Blog – weekly news/overview in the form of class blog not in news section.