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

E-SAFETY PROCEDURE

Effective Date: 01/04/2017 **Review Date:** June 2026 Biennial

Review Date	Signed Head Teacher	Signed Director RCSAT
09/09/2018		
30/09/2020		
30/05/2022		
16/06/2024		

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 procedure will operate in conjunction with other policies & procedures including those for Pupil Behaviour, Dignity & Respect, Curriculum, Data Protection and IT Acceptable Use.

1.4. This procedure applies to all RCSAT staff (including agency),pupils/students, parents/carers. Trustees, ambassadors and other volunteers.

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. Standards and Expectations

3.1. Systems

3.1.1. Academy computer systems will be configured to ensure the teaching and learning requirements of the academy are met whilst ensuring online safety is maintained.

3.1.2. Risk assessments are completed (a Data Privacy Impact Assessment, DPIA) when there is a major overhaul to the system or a new cloud-based software package is purchased, for example.

3.1.3. The system will be compliant with the academy, Trust, local authority, DfE, ICO and Data Protection guidelines with regard to online safety procedures being met.

3.1.4. Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.

3.1.5. Academy IT staff will be responsible for monitoring IT use.

3.2. Filtering & Monitoring

3.2.1. The academy will ensure an accredited filtering system is used. Filtering reports and logs will be examined regularly.

3.2.2. The academy will ensure an accredited monitoring system is used. Monitoring reports and logs will be examined regularly.

3.2.3. Any filtering incidents are examined, and action taken and recorded to prevent a recurrence. The academy will provide enhanced/differentiated user-level filtering. Internet access will be filtered for all users.

3.3. Network security

3.3.1. All users will have clearly defined access rights to academy technical systems and devices.

3.3.2. All users will be provided with a username and secure password by academy IT staff. Users are responsible for the security of their username and password.

3.3.3. The Business Manager and Executive Headteacher/other designated senior person will have access to the main administrator password.

3.3.4. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts which might threaten the security of the academy systems and data.

4. Internet Use Benefitting Education

4.1. Benefits of using the Internet in education include:

- **4.1.1.** access to world-wide educational resources including museums and art galleries;
- **4.1.2.** inclusion in the National Education Network which connects all UK schools;
- **4.1.3.** educational and cultural exchanges between pupils world-wide;
- **4.1.4.** access to experts in many fields for pupils and staff;
- **4.1.5.** professional development for staff through access to national developments, educational materials and effective curriculum practice;

4.1.6. collaboration across support services and professional associations;

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

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

4.2. Internet use enhances learning through:

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

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

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

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

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

4.3. Authorised Internet Access.

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

4.3.2. All staff, governors and volunteers shall read and sign the 'IT Acceptable Use Agreement' before using any school resource.

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

5. Use of images and videos

5.1 The academy will ensure images and videos of students, staff, students' work and any other personally identifying material are used, stored, archived, and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy (Appendix 4).

5.2 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the Internet e.g., social media sites.

5.3 Written permission from parents or from E-ACT will be obtained before photographs of students are published on the academy website/social media/local press.

5.4 In accordance with guidance from the ICO, parents are able to take videos and digital images of their children at academy events for their own personal use but should not be made publicly available where other students are involved in the digital image or video. Students must not take, use, share, publish or distribute images of others without their permission.

6. Data Protection

6.1 Personal data will be recorded, processed, transferred, and made available according to the Trust Data Protection Policy and in compliance with GDPR and the Data Protection Act (1998).

7. **World Wide Web**

7.1. 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.

7.2. RCSAT schools shall ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

7.3. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

8. **E-mail**

8.1. Pupils may only use approved e-mail accounts on the school system.

8.2. Pupils shall tell a teacher as soon as possible if they receive offensive e-mail.

8.3. Pupils shall not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

8.4. Only whole class or group e-mail addresses shall be used in school.

8.5. Access in school to external personal e-mail accounts may be blocked.

8.6. 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.

8.7. The forwarding of chain letters/chain emails is not permitted.

9. **Social Networking**

9.1. School shall block/filter access to social networking sites is blocked and filtered where possible in line with Local Authority.

9.2. Pupils shall be advised never to give out personal details of any kind which may identify them or their location.

9.3. Pupils shall be advised not to place personal photos on any social network space.

9.4. Pupils shall be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

9.5. Pupils shall be encouraged to invite known friends only and to deny access to others.

9.6. Trustees, academy, national and regional team staff, students and volunteers are expected to comply with the Trusts social media policy.

10. **Managing Emerging Technologies**

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

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

11.1. The contact details on the Web site shall be the school address, e-mail and telephone number.

11.2. Staff or pupils personal information shall not be published.

11.3. The Principal nominee shall take overall editorial responsibility and ensure that content is accurate and appropriate.

12. Responsibilities

12.1.1 The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the academy community. Headteacher should ensure that all academy staff and visitors are aware of the Online Safety Policy and procedure and of their responsibilities set out in this policy. It is the responsibility of the Headteacher to ensure that breaches of the policy are investigated and addressed.

12.1.2 Academy staff, regional and national team staff, ambassadors and trustees are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the academy into disrepute or damage their own professional reputation.

12.2 **Academy management and online safety**

12.2.1 Academy Senior Leadership Teams (SLTs) are responsible for determining, evaluating and reviewing online safety to encompass teaching and learning, use of academy IT equipment and facilities by students, staff and visitors, and agreed criteria for acceptable use by students, academy staff and trustees of Internet capable equipment for academy related purposes, or in situations which will impact on the reputation of the academy, and/or on academy premises. This is in line with expectations in Keeping Children Safe in Education in relation to an annual review/risk assessment of online safety provision.

12.2.2 Regular assessment of the strengths and weaknesses of practice within the academy will help determine INSET provision needed for staff and guidance provided to parents, students, and local partnerships.

12.3 **Online Safety Co-ordinator**

12.3.1 The academy has a designated Online Safety Co-ordinator (see individual academy website for contact details) who reports to the Senior Leadership Team and co- ordinates online safety provision across the academy and wider academy community.

12.3.2 The academy's Online Safety Co-ordinator is responsible for online safety issues on a day to day basis and also liaises with relevant stakeholders including IT support, the Trust's Safeguarding Leader, and other Trust contacts, to ensure the safety of students.

12.3.3 The Online Safety Co-ordinator maintains a log of submitted online safety reports and incidents.

12.3.4 The Online Safety Co-ordinator audits and assesses inset requirements for staff, support staff and trustee online safety training, and ensures that all staff are aware of their responsibilities and the academy's online safety procedures. The Co-ordinator is also the first port of call for staff requiring advice on online safety matters.

12.3.5 The Online Safety Co-ordinator is responsible for promoting best practice in online safety within the wider academy community, including providing and being a source of

information for parents and partner stakeholders. This may include facilitating regular assemblies and other such activities that focus on positive messages and behaviours.

12.3.6 The Online Safety Co-ordinator will be involved in any risk assessment of new technologies, services, or software to analyse any potential risks.

12.4 **Trustees and academies team**

12.4.1 The Trustees delegate a number of functions to the national teams. The Trust Safeguarding Leader, on behalf of the Board of Trustees, and the academy's Online Safety Co-ordinator will liaise directly with one another with regard to reporting on online effectiveness, incidents, monitoring, evaluation to the Executive Leadership Team (ELT) and the Education Committee and developing and maintaining links with local stakeholders and wider academy community.

12.4.2 This is important also to provide and evidence of a link between the academy, trustees, and parents.

12.4.3 The Safeguarding Leaders must ensure that they have demonstrable experience, skills and training to be able to provide appropriate challenges and support to the academy management team.

12.5 **IT support staff**

12.5.1 Internal IT support staff are responsible for maintaining the academy's networking, IT infrastructure and hardware. IT staff will be aware of current thinking and trends in IT security and ensure that the academy system, particularly file-sharing and access to the Internet, is secure. IT staff will ensure systems are not open to abuse or unauthorised external access.

12.5.2 IT support staff in academies are responsible for:

12.5.2.1 Defending the network and infrastructure of the academy, reviewing activity logs regularly;

12.5.2.2 Ensuring that users comply with basic access policies and that only trusted devices can connect to the academy network;

12.5.2.3 Filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised;

12.5.2.4 To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with the management team and Online Safety Co-ordinator;

12.5.2.5 To report to the management team and Online Safety Co-ordinator on any network intrusions or other threats to the network;

12.5.2.6 To ensure that any IT outsourced e.g., connectivity, maintenance, cloud-based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations;

12.5.2.7 Promoting basic cyber security practices within the academy e.g., locking computers when away from the desk, using secure passwords, caution when using USB removable drives.

12.5.3 External contractors, website designers/hosts will be made fully aware of and agree to the Trust's Online Safety Policy.

12.6 **All Staff**

12.6.1 Teaching and support staff are responsible for ensuring that they understand

the Trust's Online Safety Policy, practices, and associated procedures for reporting online safety incidents in line with academy procedures.

12.6.2 All staff will be provided with an online safety induction as part of the overall staff induction procedures. All staff will attend mandatory online safety training provided by the academy or the Safeguarding Leader.

12.6.3 All staff will ensure that they have read, understood, and signed the Acceptable Use Policy (Appendix 4) relevant to Internet and computer use in each academy.

12.6.4 All teaching staff are to be vigilant in monitoring student Internet and computer usage in line with the policy. This may include the use of personal technology, such as cameras and phones on the academy site where there is a cause for concern.

12.6.5 Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

12.6.6 Staff must promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents.

12.6.7 Staff must report as soon as is practicable any suspected misuse of Trust/academy digitally connected systems to the Headteacher or Online Safety Co-ordinator.

12.7 **Designated Safeguarding Lead (DSL) The DSL**

12.7.1 Will hold the lead responsibility for online safety, within their safeguarding role.

12.7.2 Will be trained in specific online safety issues e.g., CEOP accredited course or equivalent.

12.7.3 Will be responsible for escalating online safety incidents to the relevant external parties e.g., CEOP, Cyber Choices, National Cyber Security Centre, local Police, Local Safeguarding Children's Board, social care and parents/E- ACTs, ELT. Possible scenarios might include:

12.7.3.1 Allegations against members of staff;

12.7.3.2 Cybercrime – illegal hacking, denial of service, use of malware;

12.7.3.3 Allegations or evidence of 'grooming;'

12.7.3.4 Allegations or evidence of cyber bullying in the form of threats of violence, harassment, or a malicious communication;

12.7.3.5 Sharing of indecent images including nudes or semi-nudes (consensual or non-consensual) [OBJ];

12.7.3.6 Sexual violence or harassment between peers (peer on peer abuse).

12.7.4 Is responsible for acting 'in loco parentis' and liaising with websites and social media platforms, such as Twitter and Facebook, to remove instances of illegal material or cyber bullying.

12.8 **Pupils/Students**

12.8.1 Pupils/students must ensure use of academy Internet and computer systems in agreement with the terms specified in the policy. In secondary phases, students are expected to sign the policy to indicate agreement.

12.8.2 Students are responsible for ensuring they report online safety incidents in the academy or with other external reporting facilities, such as CEOP or Childline, and are expected:

12.8.2.1 To be aware of and comply with academy policies for Internet and mobile technology usage in the academy, including the use of personal items such as mobile

phones;

12.8.2.2 To be aware that their Internet use out of the academy on social networking sites, is covered under the Online Safety Policy if it impacts on the academy and/or its staff and students in terms of cyber bullying, reputation, or illegal activities;

12.8.2.3 To follow basic cyber security practices within the academy e.g., locking computers when away from the desk, using secure passwords, caution with use of USB removable drives.

12.9 **Parents/Carers**

12.9.1 Parents/carers must support the academy in its promotion of good Internet behaviour rand responsible use of IT equipment and mobile technologies both at the academy and at home.

12.9.2 Where appropriate, parents should sign the academy's Acceptable Use Policy (Appendix 4), indicating agreement regarding their child's user and also their own use with regard to parental access to academy systems such as websites, forums, social media, online reporting arrangements and questionnaires.

5.11 Remote Education

5.11.1. Academies will have due regard to the DfE's 'Providing remote education: guidance for schools[2]' after the expiration of the temporary provisions in the Coronavirus Act 2020 in relation to remote education.

6. Working from home / outside of the Academy

6.1 Working from home and accessing personal data from outside of the academy presents risks we need to be aware of to keep staff, students and their data safe.

6.2 Staff members must use secure passwords and keep these safe. They must not be accessible by others.

6.3 Devices must always be locked when not in use.

6.4 Staff must only use official communication channels when communicating personal i nformation about staff and students such as the academy email and Microsoft Teams.

6.5 Staff using academy devices for academy work should always use this for accessing academy data and websites. This device should have appropriate controls and safeguards in place to ensure that data is kept secure. Academy devices are for academy employees only and should not be used by any other members of the family or household.

6.6 Staff should not use personal devices for work-related activity.

6.7 Staff and students should always be aware of Phishing e-mails and should pay particular attention to the following:

- senders email address that does not match the organisation's address.
- spelling / grammatic mistakes
- Urgency in requests for action
- Requests to input personal credentials

6.8 Staff and students should not save any personal data onto removable media (USB drives, CDs etc) and instead use the approved tools and services already provided by the trust. Files and resources can be saved to One Drive through the Office 365 portal https://portal.office.com

6.9 Staff and students must stay alert and report anything that they are

unsure of. If something looks or seems not right, it probably is not.

13 **Assessing Risks**

13.1 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.

13.2 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.

14 **Handling E-Safety Complaints**

14.1 The Principal shall deal with complaints of Internet misuse.

14.2 Any complaint about staff misuse shall be referred to the Principal.

14.3 Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.

14.4 Pupils and parents shall be informed of the complaints procedure.

15 **Review**

15.1 This procedure will be monitored and reviewed every 2 years.

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	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, newsletters, PTA, general school events e.g. parents evening dates
- Policies and Website layout – Resources RCSAT
- News Page – for specific events e.g. fundraising activities
- Teachers Class Page – update regularly with general info, topic overview, photos
- The schools Principals have editorial responsibility for their school's webpages ensuring content is up to date and in line with policy

Appendix 4 IT Acceptable Use

Introduction

ICT in its many forms – internet, email, mobile devices etc – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly.
All staff and Governors of Rural Church Schools Academy Trust are aware of the following responsibilities:

- All Staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.

- All staff, Governors and visitors understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner.

- No staff, Governors or visitors will disclose any passwords provided to them by the school.

- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username.

- Staff, Governors and visitors will not install any hardware or software on any school owned device without the Headteacher/Principal permission.

- All staff, Governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it to the Headteacher/Principal as soon as possible.

- All staff, Governors and visitors will only use the school's email / internet and any related technologies for uses permitted by the Headteacher/Principal. If anyone is unsure about an intended use, they should speak to the Headteacher/Principal beforehand.

- All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Headteacher/Principal or Governing Body. No passwords should be divulged and laptops/memory sticks will be encrypted.

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All staff, Governors and visitors will only use the approved email system for school business.

- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used in our brochure or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used. Filming and photography by parents and the wider community at school events, such as sports days and school productions are the responsibility of parents and not the school. School is not responsible for images that may appear on social media which have been posted by parents or carers. When possible, a professional photographer will come to school to take photographs of children, for example in their play costumes. These will then be made available to parents.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head/Principal or Pastoral Manager with our school's Safeguarding Policy.

Specific Do's and Don'ts for IT Use are detailed here:

DO transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
DO use secure portable computing devices i.e encrypted laptops or encrypted USB's when working remotely or from home.
DO use Onedrive on Office 365 to store documents securely, you can access these from any location on any device with a secure internet connection, save the changes in onedrive and not on your device.
DO use Security Pin Numbers on all staff ipads and personal mobile devices that are used for work emails, eg mobile phone.
DO Log out or lock your PC or laptop when you leave your desk; **DO** only use your allocated work email address as it is secure; **DO** use Egress Switch for emailing personal data about a child;
DO use pseudonyms and anonymise personal data where possible.
DO ensure that access to SIMS, Teachers2parents (and equivalent programs) are restricted to appropriate staff only and that leavers are removed in a timely manner

DO NOT put a forward on your work email to your personal email;
DO NOT open any attachments on suspicious emails or where you do not know who the sender is, delete from your system and report to the Data Protection Officer;

DO NOT use any pictures of children where they have their faces blurred out;
DO NOT unnecessarily copy other parties into e-mail correspondence.
DO NOT e-mail documents to your own personal computer.
DO NOT store work related documents on your home computer.
DO NOT leave documentation or laptops in vehicles overnight.
DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.
DO NOT use unencrypted memory sticks or unencrypted laptops

I acknowledge I have received and understood the IT Acceptable Use Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by RCSAT. Any failures to follow the policy can therefore result in disciplinary proceedings.

Full Name _____

Signature _____

Date _____