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

E-SAFETY POLICY

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		
12/06/2024		

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 policy will operate in conjunction with other policies including those for Pupil Behaviour, Dignity & Respect, Curriculum, Data Protection and Security.

1.4. This policy applies to any individual who is given access to RCSATs digitally connected systems (including email addresses and any other data source or system that is hosted/operated/controlled remotely or other by the organisation)

1.5. RCSAT expects all academies will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the internet both on and off the academy site. This will include imposing rewards and the sanctions for behaviour- as defined as regulation or student behaviour under the Education and Inspections Act 2006. The 'In loco parentis' duty allows the academy to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites and hosting providers on behalf of pupils.

1.6. As identified by keeping children safe in education, this policy recognises that technology plays a significant role in children's lives and abuse can take place concurrently online and in daily life. Online safety must therefore be considered as part of a whole academy approach

2. Rights Respecting Schools

2.1. The RRSA (Rights Respecting Schools Award) is given by a charity called UNICEF (United Nations International Children's Emergency Fund) . UNICEF works hard to help children and families all over the world. It works hard to ensure that all children can enjoy their rights by upholding the UNCRC. We all have rights and they cannot be taken away from us.

2.2. Bunbury Aldersey Gold and St Oswald's Silver are Rights Respecting award Schools because we want our schools to become a better place for everyone. We want to teach children about their rights and we want them to understand how to respect each other's rights. Rights Respecting Learning makes us think more about other people all over the world and how our actions and words affect them. Warmingham have decided to become a Rights Respecting School and are working towards bronze.

2.3. The ethos created in the schools works in unison with our mission statements as Church of England Schools and demonstrates to the children the inclusiveness of being a rights-respecting school.

3. Good Habits

3.1. E-Safety depends on effective practice at a number of levels:

3.1.1. Responsible IT use by all staff and pupils; encouraged by education and made explicit through published policies.

3.1.2. Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

3.1.3. Safe and secure broadband from Cheshire East Council for Learning including the effective management of content filtering.

3.1.4. National Education Network standards and specifications.

4. E –Safety Policy

4.1. RCSAT will appoint a Pastoral Manager, detailed in Appendix 1.

4.2. In RCSAT Schools the Co-ordinators will liaise with the Designated Safeguarding Leads.

4.3. The online safety policy covers the use of:

- Academy based IT systems and cloud-based software
- Academy based intranet and networking

- Academy related external internet, including but not exclusively, extranet, e-learning platforms, blogs, social media, websites
- External access to internal academy networking, such as webmail, network access, file-serving (document folders) and printing
- Academy IT equipment off site, for example staff laptops, digital cameras, mobile phones, tablets, dongles

4.4. The definition of an online incident is:

'any *incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress caused to another person or the reputation of the Academy and/or RCSAT. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages, or other means:'*

4.4.1 The most likely areas of risk to students are:

CONTENT: exposure to illegal inappropriate or harmful material; being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

CONTACT: Subject to harmful online interaction with other users; being

Subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

CONDUCT: The individual's personal online risky behaviour that then leads to harm; online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (eg consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

COMMERCE. Online 'commerce' (online gambling, inappropriate advertising, phishing, or financial scams); commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

5. Implementation

5.1. The Board of Trustees of the RCSAT has delegated for the implementation of this policy through written procedures to the Executive Headteacher and Principals within the RCSAT.

5.2. The procedure for E-Safety is included in procedure RCSAT-PR-027-01.

5.3. The Board of Trustees of the RCSAT retains overall responsibility for actions by any and all schools within the RCSAT.

5.4. RCSAT actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students, staff and the Trust and associated academies and their reputations. We seek to promote a 'cyber aware' culture that ensures all staff, students and Trustees take part in and continue to develop their knowledge and understanding of online behaviour and in particular, how to prevent harm through continual learning resources, research, and encouragement from all teachers.

6. Governors Responsibility

6.1. To ensure that the Board of Trustees and Principals have undertaken all procedures in line with the Behaviour Policy and Procedures to support the child and parents.

6.2. To consider the arrangements for continued education for the excluded pupil, parents' representations, and clear management of records to support their decision.

7. Review

7.1. The Board of Trustees reviews this policy every two years.

7.2. The governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the Board of Trustees receives recommendations on how the policy might be improved.