E-Safety Policy

Name of Policy	E-SAFETY POLICY
Policy Level	RFSS Local Policy
Date of issue	March 2024
Author:	Rugby Free Secondary School
Date of Next Review:	March 2025
Date of Approval:	March 2024

Table of Contents

1. Policy Aim

Our students are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also several challenges and risks. The use of the latest and most cutting-edge technology is actively encouraged at Rugby Free Secondary School, however with this comes a responsibility to protect students to ensure they remain safe online.

Online safety is an integral part of safeguarding. This policy is written in line with the DfE statutory guidance 'Keeping Children Safe in Education' 2023 updates (KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy. The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

2. School E-Safety Aims

RFSS aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver and identify approaches to educate and raise awareness to E-safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (mobile phones)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Identify clear procedures to use when responding to e-safety concerns.

3. The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

- Contact – being subjected to harmful online interaction with other users, such as 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 – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

4. Using Technology

RFSS and Learning Today Leading Tomorrow Trust (LT2) acknowledge that technology can improve the planning, managing workload and delivery of teaching as well as making the learning experience more dynamic and interactive for students. Therefore, RFSS will support the best accountable practice for embedding effective use of technology in teaching and learning.

RFSS and LT2 recognise that all professionals need to use technology to enhance their working practice and develop innovative ways of personalising learning to suit the different aptitudes and interests of learners, including those with special educational needs.

Whilst technical solutions must be put in place to ensure that users are not exposed to risk, it is also key to prepare young people to be safe and responsible users of technology in the world outside of school.

5. Roles and Responsibilities

5.1 All Staff

All staff are expected to:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) is
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education 2023 (whilst Part 1 is statutory for all staff, Annex A for Senior management team and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum leads / subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for students)
- Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc.) in school or setting as homework tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- Carefully supervise and guide students when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage students to follow their acceptable use policy, including the remote learning responsible user agreement for students, remind them about it and enforce school sanctions
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment

- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors and other communal areas outside the classroom and let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Follow the remote learning policy and teacher protocols during any part or full school closure, in line with the Remote Learning Policy.

5.2 Headteacher and LT2

The Headteacher and Trust are expected to:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance
- Liaise with the designated safeguarding lead and online safety coordinator on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DSL, Proprietor and senior leadership team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always

put first and data-protection processes support careful and legal sharing of information.

- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles, inlcuding monitoring and filtering as KCSiE 2023 outlines
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g., network manager) who carry out internal technical online-safety procedures
- Ensure the Proprietor is regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure all remote learning policies are kept up to date
- Ensure the school website meets statutory requirements

5.3 Designated Safeguarding Lead

The Designated Safeguarding Lead is expected to:

- Liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Headteacher, and Senior Leadership Team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety

- Review and update this policy, other online safety documents (e.g. Acceptable Usage Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the Headteacher
- Receive regular updates on online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated advisory board member for child protection to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss filtering and monitoring.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Ensure that up to date Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff

5.4 ICT Manager

The ICT Manager is expected to, as listed in the 'all staff' section, plus:

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety coordinator to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal

and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.

- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and SLT
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy

5.5 Leader of Digital Communications Department

The Leader of Digital Communications Department is expected to as listed in the 'all staff' section, plus:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements, including remote learning agreements.

5.6 Students

Students are expected to:

- Understand the importance of reporting abuse, misuse or access to inappropriate materials

- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies (including remote learning policies) cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing e-safety issues

5.7 Parents / Carers

Parents and Carers are expected to:

- Read, sign and promote the school's parental acceptable use policy (AUP), Including remote learning policies and read the student AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, Proprietor, contractors, students or other parents/carers.
- Seek support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online
- Use school systems, such as learning platforms, and other network resources, safely and appropriately
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

5.8 National Curriculum Expectations

Students in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- Students begin Year 7 with a unit on e-safety as part of the Digital Communications curriculum

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- How to report a range of concerns

By the end of secondary school, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

6. Online Bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.
All forms of bullying are recorded on the school's safeguarding software: CPOMS.
The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7. Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

8. Using the Internet

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. This is done by utilising online monitoring software such as Senso Cloud and Impero.

9. Password Policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

From Year 7, all students are provided with their own unique username and private passwords to access our systems; students are responsible for keeping their password private.
We advise/require all users to:

- Use strong passwords for access into our system
- Change their passwords regularly
- Always keep their password private; users must not share it with others or leave it where others can find it
- Not login as another user at any time

10. Students Using Mobile Devices

Students may bring mobile devices into school; however they are not permitted to use them during:

- Lessons (Apart from logging information during PSHE lessons)
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Phones must not be seen or heard. Any breach of the acceptable use agreement by a student action will be taken in line with the school's Relationship for Learning Policy.

11. Staff using work devices outside school

All staff members at RFSS will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g., asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from Trust Strategic IT Manager.

12. How the school will respond to issues of misuse

Where an RFSS student misuses the school's ICT systems or internet, we will follow the procedures set out in our acceptable use policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

RFSS will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

All new RFSS staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. Staff will be informed of their responsibilities regarding monitoring and filtering.

All RFSS staff will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who do not want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

RFSS staff will then:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements

The DSL will log behaviour and safeguarding issues related to online safety, using CPOMS and Impero.

This policy will be reviewed every year. At every review, the policy will be shared with the Trustee board.

15. Links with other policies

This policy links with several other policies, practices and action plans including:

- Relationship for Learning Policy
- Remote Learning Policy
- Data Protection Policy
- Curriculum Policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Child Protection and Safeguarding Policy