Online Safety Policy

Approved by	**RET Board**	Approved on	**September 2021**
SLT contact	**CEO/Safeguarding Adviser**	Revision due	**Every 2 years**

RUSSELL EDUCATION TRUST

1. Aims

Our school aims to:

a. Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
b. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
c. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
d. Our approach to online safety is based on addressing the following four key categories of risk:
    1. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
    2. **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
    3. **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; and
    4. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

a. This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
    1. Teaching online safety in schools
    2. Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
    3. Relationships and sex education
    4. Searching, screening and confiscation
    5. Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
    6. Sexual violence and sexual harassment between children in schools and colleges
    7. Working together to safeguard children
    8. It also refers to the DfE's guidance on protecting children from radicalisation.
b. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.
c. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

a. The Trust Board and Local Governing Body
    1. The Local Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
    2. The Local Governing Body will co-ordinate meetings with appropriate staff to discuss online safety.
    3. All trustees and school governors will:
        - Ensure that they have read and understand this policy
        - Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
        - Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

b. The headteacher
   1. The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

c. The designated safeguarding lead
   1. Details of the school's DSL and DSLs are set out in our safeguarding and child protection policy as well as relevant job descriptions.
   2. The DSL takes lead responsibility for online safety in school, in particular:
      - Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
      - Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
      - Managing all online safety issues and incidents in line with the school child protection policy
      - Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
      - Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
      - Updating and delivering staff training on online safety
      - Liaising with other agencies and/or external services if necessary
      - Providing regular reports on online safety in school to the headteacher and/or governing board
      - Provide training for staff on online safety
      - Alongside other senior leaders, ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour policy and anti-bullying policy
      - This list is not intended to be exhaustive.

d. The ICT manager
   1. The Trust ICT manager is responsible for:
      - Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students and staff are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
      - Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
      - Conducting regular security checks and monitoring the school's ICT systems
      - Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
      - Support in the investigation of any incidents of cyber-bullying
      - This list is not intended to be exhaustive.

e. All staff and volunteers
   1. All staff, including contractors and agency staff, and volunteers are responsible for:
      - Maintaining an understanding of this policy
      - Implementing this policy consistently
      - Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (Appendix 1)
      - Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
      - Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
      - Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
      - This list is not intended to be exhaustive.

f. Parents
   1. Parents are expected to:
      - Notify a member of staff or the headteacher of any concerns or queries regarding this policy
      - Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
   2. Parents can seek further guidance on keeping children safe online from the organisations detailed on the school's website.

g. Visitors, trainees and members of the community
   1. Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

a. Students will be taught about online safety as part of the curriculum:
b. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.
c. All secondary schools have to teach:
   1. Relationships and sex education and health education 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
   2. 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
   3. 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 PSHCE and 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.

5. Educating parents about online safety

a. The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.
b. Online safety will also be covered during parents' evenings and/or parents' seminars and information events.
c. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
d. Concerns or queries about this policy can be raised with the DSL or the headteacher.

6. Cyber-bullying

a. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the behaviour policy.)

7. Preventing and addressing cyber-bullying

a. 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.
b. 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. Class teachers and form teachers will discuss cyber-bullying with their tutor groups.
c. 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.
d. All staff, governors and volunteers (where appropriate) receive training and/or updates on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).
e. 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.
f. 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.
g. 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.

8. Examining electronic devices

a. 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.
b. Protocols for examining student devices are contained in the DfE and Trust guidance documents for conducting searches.
c. 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:
    1. Cause harm, and/or
    2. Disrupt teaching, and/or
    3. Break any of the school rules
d. If inappropriate material is found on the device, it is up to the DSL in conjunction with the Headteacher to decide whether they should:
    1. Delete that material, or
    2. Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

3. Report it to the police (staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.)

e. Any searching of students will be carried out in line with:
   1. The DfE's latest guidance on screening, searching and confiscation
   2. UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
   3. The school's COVID-19 risk assessment

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

9. Acceptable use of the internet in school

a. 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 (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
b. 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.
c. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
d. More information is set out in the acceptable use agreements in appendices 1, 2.

10. Students using mobile devices in school

a. Students may bring mobile devices into school, but are not usually permitted to use them during:
   1. Lessons
   2. Tutor group time
   3. Clubs before or after school, or any other activities organised by the school
b. Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendices 1 and 2).
c. Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

11. Staff using work or personal devices

a. All staff members will take appropriate steps to ensure their personal devices remain secure. This includes, but is not limited to the following measures which are applied to school devices:
   1. 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)
   2. 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
   3. Making sure the device locks if left inactive for a period of time
   4. Not sharing the device among family or friends
   5. Installing anti-virus and anti-spyware software
   6. Not leaving the device unattended in a public place or visible in a locked vehicle.
   7. Keeping operating systems up to date – always install the latest updates
   8. Staff members must not use school devices or services/systems in any way which would violate the school's terms of acceptable use, as set out in appendix 2.
   9. Work devices must be used solely for work activities.
   10. If staff have any concerns over the security of their devices, they must seek advice from the school.

12. How the school will respond to issues of misuse

a. Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour, Safeguarding and Child Protection, Anti-Bullying and ICT Acceptable Use The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
b. 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 staff disciplinary policy and/or the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
c. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

a. Staff members will receive training on safer internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
b. All staff members will receive refresher safeguarding training at least once each academic year, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
c. By way of this training, all staff will be made aware that:
    1. Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
    2. 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 don't want to receive such content
        - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element
    3. Training will also help staff:
    4. develop better awareness to assist in spotting the signs and symptoms of online abuse
    5. develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
    6. develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term
d. The DSL and DDSLs 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.
e. Governors will receive updates on safe internet use and online safeguarding issues.
f. Volunteers will receive appropriate training and updates, if applicable.
g. More information about safeguarding training is set out in our safeguarding and child protection policy.

14. Monitoring arrangements

a. The DSL or DDSL logs behaviour and safeguarding issues related to online safety on CPOMS.
b. This policy will be reviewed every year by the Trust. At every review, the policy will be shared with the Trust Board. The review will be supported by an annual risk assessment for the school written by the Headteacher and DSL that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.