Rose Education Provision

E-Safety Policy

August 2025

1. Aims

At Rose Education Provision we:

- Have robust processes in place to ensure the online safety of students, staff and volunteers
- 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')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety at Rose Education Provision 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, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child to child 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2024)and its advice for schools on:

- Teaching online safety in schools (DFE 2023)
- Preventing and tackling bullying (DFE 2017)
- Relationships and sex education (RSE) and health education (DFE 2021)
- Searching, screening and confiscation: advice for schools (DFE 2022)

It also refers to the DfE's guidance on Protecting Children from Radicalisation: The Prevent Duty (DFE 2022).

It reflects existing legislation, including but not limited to the Education Act 2011 , 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.

The policy also considers the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) is Miss Sheree Curtis

The DSL takes lead responsibility for online safety in school and in particular for:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with partnership schools, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the college's Safeguarding and Child Protection policy
- Ensuring that any online safety incidents are logged immediately and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged 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
- Referring to the Cyber Choices national programme for reducing cybercrime, as appropriate

3.2 All staff and volunteers

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 and ensuring that students follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged immediately 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'
- Any form of Cyber Crime, both deliberate and inadvertent

NOTE: This list is not intended to be exhaustive.

3.3 Parents/Carers

Parents are expected to:

- Notify a member of staff or the head of school of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms of e-safety policy

Parents can seek further guidance on keeping children safe online from the following oranisations and websites:

- UK Safer Internet Centre https://saferinternet.org.uk/
- NSPCC-Keeping children safe online https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- Kidscape https://www.kidscape.org.uk/training/online-safety-and-cyberbullying-awareness-for-parents-and-carers/
- Thinkuknow https://www.thinkuknow.co.uk/parents/
- South West Grid for Learning (SWGFL) www.swgfl.org.uk
- National Cyber Security Centre www.ncsc.gov.uk/section/information-for/individuals-families

4. Educating students about online safety

Students will be taught about online safety as part of the PHSE curriculum:
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 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 recognize consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- About different types of cybercrime and the dangers of them, both inadvertent and deliberate.

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

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is described as '**several times on purpose'** with the intention of harming a person or groups by another person or group, where the relationship involves an imbalance of power. (See the school anti-bullying policy).

5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, at Rose Education Provision 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.

We will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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 and volunteers (where appropriate) will receive training on cyber-bullying, its impact and ways to support students, as part of the college's safeguarding training programme.

In relation to a specific incident of cyber-bullying, we will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, we will contact the relevant external agencies ie the Police or Children's Social Services

The Designated Safeguarding Lead or a member of the safeguarding team will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

5.3 Examining electronic devices

The Head of School and authorised members of staff (Rose Education Provision's Behaviour Policy 2025), will carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff members will:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation.

If it is known, or alleged, that there is inappropriate material on a device, the head of school or, Designated Safeguarding Lead will confiscate the device from the student and take appropriate action in line with the college's Behaviour Policy (2025) the DFE's latest guidance on Screening, searching and confiscation (DFE 2024), Keeping Children Safe in Education (2024) and the UK Council for Internet Safety (UKCIS) guidance "Sharing nudes and semi-nudes-advice for education settings working with children and young people".
If there are images, data or files on a device that any member of staff reasonably suspects are likely to put a person at risk, they **must not** view the image or any other content and immediately report the concern to the Designated Safeguarding Lead or a Deputy Safeguarding Lead will act immediately and accordingly.

7. Acceptable use of the internet in school

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.

staff

● Any internet use will be planned to ensure that it is age appropriate and supports the learning objective for specific topics.

● When searching the internet for information, students will be guided to use age appropriate search engines. All use will be monitored and students will be reminded of what to do if they come across unsuitable content.

● Students will be made aware of the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.

● Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as NSPCC.

Students

Students Publishing Content Online

● Students will not be allowed to post or create content on sites unless the site has been approved by management

● Students' full names will not be used anywhere on the website, particularly in association with photographs and videos.

● Written permission is obtained from the parents/carers before photographs and videos are published.

● Any images, videos or sound clips of students must be stored on the Rose Education drive and not on personally owned equipment.

● Students and staff are not permitted to use portable devices to store images/video/sound clips of students.

8. Students using mobile devices in school

Students who need to bring a mobile phone in to Rose Education are permitted to do so but:

● The phone should be kept away and switched to silent during the lessons

● Students should be encouraged not to use phones during their sessions wherever possible. However, we do realise that due to the nature of the conditions of some of the students we work with, their phones can be very important to them and offer a means of security and comfort and a distraction from anxiety

9. Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if a staff member has good reason to suspect the device may be used to:

● cause harm

● disrupt sessions,

● commit an offence,

● cause personal injury,

● damage property

9. Staff using work devices outside school

All staff members at Rose Education Provision will take appropriate steps to ensure their devices remain secure.

This includes, but is not limited to:

- Keeping the device password-protected – strong passwords in line with current password guidance.
- If using a hard drive ensuring that the hard drive is encrypted.
- Locking the device when not using it, even for a brief period of time
- Not sharing the device with family or friends
- Not sharing or placing in clear view, usernames and passwords (electronically or hand written). Where passwords and usernames need to be emailed then two forms of separate communication should be adhered to.
- Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in policy.
- Work devices must be used solely for work activities. No personal photo's or documents to be stored on school network devices. School email should not be used for personal communication.

9. Staff use of personal device

● Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity. All contact must be done through the designated Rose Education phone.

● If a member of staff breaches the policy then disciplinary action may be taken.

•Social networking

staff will not post content or participate in any conversations which will be detrimental to the image of Rose Education. Staff who hold an account should not have parents or students as their 'friends'. Doing so will result in disciplinary action or dismissal

. ● Blogs or social media sites should be password protected and run from the Rose Education Website with approval from Director

10. How the school will respond to issues of misuse

Where a 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 college'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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new 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.

Every member of staff, volunteer and each governor will receive safeguarding refresher training at the start of each academic year and on-going safeguarding training throughout the academic year as part of the safeguarding training programme, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all adults 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 other children 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

Training will also help adults to:

- 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 up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The Designated Safeguarding Lead will undertake appropriate up-to-date online safety training on a regular basis.

The DSL will undertake child protection and safeguarding refresher 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.

Volunteers will receive safeguarding refresher training at the start of each academic year and on-going safeguarding training throughout the academic year as part of the safeguarding training programme.

12. Radicalisation procedures and monitoring

Radicalisation Procedures and Monitoring It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we are located. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Designated Safeguarding Lead). All students must be fully supervised when accessing the internet.

12. Sexual Harassment

Sexual Harassment Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include non-consensual sharing of sexual images and videos, inappropriate sexual comments on social media, exploitation, coercion and threats. Any reports of online sexual harassment will be taken seriously, and the police and Children's Services may be notified. Rose Education follows and adheres to the national guidance

Response to incidents of concern

Responses to Incidents of Concern An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and students have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. Rose Education has incident reporting procedures in place and record incidents of concerns regarding e-Safety.

● All incidents of concern should be written down, signed and dated and given to the DSL as soon as possible

● At every stage the child should be involved in or informed of the action taken

● If necessary, refer to the other related internal policies e.g. Anti-Bullying, Acceptable use

12. Monitoring arrangements

Any online safety incidents will be reported immediately to a member of the safeguarding team at Rose Education Provision will take immediate action.

This policy will be reviewed every year by the Designated Safeguarding Lead.

13. Links with other policies

This policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour policy
- Anti-Bullying Policy
- Acceptable Use Policy

Author:	Miss Sheree Curtis (Head of School)		
Date:	August 2025		
Signed	*S. Curtis*	Review Date:	**August 2026**