Online Safety Policy

Prepared in Consultation with:	Sweyne Park School LGB
Last reviewed on:	September 2024
Approved by Rayleigh Schools Trust:	October 2024
Next review by:	Autumn 2024

Contents

It reflects existing legislation, including but not limited to:

The Education Act 1996 (as amended)

The Education and Inspections Act 2006, which empowers Headteachers to such extent as it reasonable, to regulate the behaviour of pupils/students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place

The Voyeurism (Offences) Act 2019

The UK General Data Protection Regulation (UK GDPR)

The Dat

The policy takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

4: Roles and responsibilities

4.1: The Local Governing Bodies (LGBs)

The LGBs have overall responsibility for monitoring this policy and holding the headteacher and other relevant staff to account for its implementation.

The LGB will review this policy annually and recommend its ratification to the Board of Trustees

The LGat

All Governors will:

- Ensure they have read and understood this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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.

4.2: The Headteacher

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

The Headteacher is also responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policy and procedures, including those relating to the curriculum, safeguarding and training.
- Supporting the DSL and DDSLs by ensuring that they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up to date and appropriate online safety training as part of their induction and ongoing safeguarding training.
- Communicating regularly with parents to reinforce the importance of children being safe online. Ensuring that parents are kept up to date with current online safety issues and how the school is keeping pupils/students safe.
- As part of the shortlisting process, consider carrying out an online search as part of due diligence on shortlisted candidates to help identify any incidents or issues that may have happened, and are publicly available online which the school might want to explore with applicants at interview.
- Working with the DSL and LGB to review this policy annually and ensure the procedures7-USwith the DS

Ensuring that any incidents of cyber-bullying are logged and dealt with in line with the school behaviour policy.

Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.

Updating and delivering staff training on online safety.

Working with the Headteacher to ensure that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.

Liaising with other agencies and/or external services if necessary.

Providing regular reports on online safety to the Headteacher and/or LGB, and meet regularly with the Governor responsible for online safety.

Undertaking annual risk assessments that consider and reflect the risks children face.

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

4.4: The Network Manager

The Network Manager is responsible for:

Providing technical support and perspective to the DSL and Headteacher, especially in the development and implementation of appropriate online safety policies and procedures.

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school networks and school devices, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe fro.-

Schools in the Rayleigh Schools Trust will raise parents/carers' awareness of internet safety through the schools' newsletters and in information via our website. This policy will also be shared with parents through the school website. Parents/carers will also be requested to read our acceptable use policies and discuss the implications with their children.

The schools will let parents/carers know:

- What systems the schools use to filter and monitor online use.
- Who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL. Concerns or queries about this policy can be raised with any member of staff.

5.3: Training for staff, volunteers, and Governors/Trustees

It is essential that staff receive online safety training and understand their responsibilities, as outlined in this policy.

All new staff receive online safety training as part of the induction programme, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation, and will be provided with this policy.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (e.g., through staff bulletins and CPD sessions). The DSL ensures that all safeguarding training given to staff includes elements of online safety, and through this

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

6: Dealing with online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment, or exploitation, whether

The internet, particularly social media, can be part of the causation of a number of mental health issues in pupils.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupils'

Pose a risk to staff or pupils, 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, if the authorised member of staff is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher, Deputy Headteacher (Behaviour) or DSL.
Explain to the pupil why they are being searched, how to search will happen, and give them the opportunity to ask questions about it.
Seek the pupil's co-operation.

Authorised members of staff may examine and in exceptional circumstances erase, any data or files on an electronic device where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

Cause harm, and/or
Undermine the safe environment of the school or disrupt teaching, and/or
Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the SLT to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member suspects that a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

Not view the image.
Confiscate the device and report to incident to the DSL immediately, who will decide what to do next.
The DSL will make the decision in line with the school's Child Protection and Safeguarding Policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the schools' complaints procedures.

7: Safer Use of Technology

All pupils/students, parents/carers, staff, volunteers and Governors/Trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet prior to being granted use of the school's network (see appendices 1 to 3). 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.

minimum and maximum length and require a combination of letters, numbers, and special characters to ensure that they are as secure as possible. Staff are required to change their passwords every 120 days.
Users must inform the Systems Manager if they forget their login details, who will arrange for the user to access the system under different login details. Users are not permitted to share their private login details with others and are not allowed to log in as another user at any time.

Staff should report to the Headteacher if they consider that any content shared or posted conflicts with their role in the Rayleigh Schools Trust

Staff are not permitted to communicate with pupils/students or their parents/carers over social networking sites and are reminded that they should alter their privacy settings to ensure pupils and parents/carers are not able to contact them on social media. Staff are also advised not to communicate with past pupils/students or their family members via social media. If ongoing contact with pupils is required once they have left the school(s), staff will be expected to use school-provided communication tools. Any pre-existing relationships that would affect this should be discussed with the Headteacher or DSL. If communication is received from pupils or parents/carers on personal social media accounts, this should be reported to the DSL, or another member of the Leadership Team.

Pupils

Pupils are taught about the safe and responsible use of social media through the CPRE, Computer Science and safeguarding curriculums, and through assemblies.

In particular, pupils/students are advised:

To consider the risks of sharing personal details of any kind on social media which may identify them and/or their location (e.g., full name, address, phone numbers, school attended, email address, specific interests, clubs). They are also advised to consider the information conveyed by photographs.

Not to meet any online friends without the permission of their parent/carer and ideally when they are present.

About appropriate security on social media, to use safe passwords, deny access to unknown individuals.

To block and report unwanted communications.

To approve and invite only known friends on social media and to deny access to others by making profiles private / protected.

Concerns regarding the online conduct of a member of staff on social media are reported to the Headteacher;

10: How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow our procedure set out in our Behaviour Policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Appendix 2: KS2, KS3, KS4 and KS5 acceptable use agreement (pupils and parents/carers)

Appendix 3: acceptable use agreement for staff, Governors,

~ I will adhere to any responsibility I have for monitoring pupils' use of technology. I will ensure that I report misuse or breaches of this agreement by pupils or staff members using the appropriate channels.
I understand that my use of Rayleigh Schools Trust systems and devices including the internet will be monitored. I understand that violations off this agreement will be dealt with in line with the appropriate policy and that disciplinary action may be taken in accordance with the Disciplinary Policy and Procedures.