Contents

1: Introduction

Rayleigh b BDC qsETQef1 0 0 1

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 outside the school, but is linked to membership of the school.

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 pupils' electronic devices where they believe there is a 'good reason' to do so. This will only be undertaken over issues covered by the schools' Behaviour Policy.

The Equality Act 2010.

The Voyeurism (Offences) Act 2019

The UK General Data Protection Regulation (UK GDPR)

The Data Protection Act 2018

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 LGB will ensure that the DSL's remit includes online safety.

The LGB will ensure that all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The LGB will also ensure that all staff receive regular online safety updates (via staff bulletin, briefings and training sessions) as required and at least annually, to ensure that they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The LGB should ensure that children are taught how to keep themselves and others safe, including keeping safe online.

The LGB must ensure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The LGB will review the DFE filtering and monitoring standards, and discuss with ICT staff and service providers what needs to be done to support the school in meeting those standards, which include:

Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

Reviewing filtering and monitoring arrangements at least annually;

Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

Having effective monitoring strategies in place that meet their safeguarding needs.

This is provided by the Trust for both schools.

The Governor

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 procedures and implementation are updated and reviewed regularly.

In addition, the Headteacher (as well as the Deputy Headteacher(s) and DSL) will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

4.3: The Designated Safeguarding Lead

The DSL takes lead responsibility for online safety at each school (supported by the Safeguarding Team of DDSLs), 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 and LGBs to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly. Policies are approved by the Board of Trustees.
- Undertaking training so that they understand the risks associated with online safety and can recognise the additional risks that children with SEND face online.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school networks and school devices.
- Working with the Systems Manager to make sure the appropriate systems and processes are in place.
- Working with the Headteacher, Systems Manager and other staff (such as the SENDCo), as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and [illegible]

Pupils/students will be expected to know the policies on the use of mobile phones. They should also know the policies on the taking/use of images and cyber-bullying.

Pupils/students should understand the importance of adopting good online safety practice when using digital technologies and realise that the school's online safety policy covers their actions outside school, if related to their membership of the school

4.8:

Pupils 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, pupils 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 that carries severe penalties including custodial sentences.

How information and data are 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. This includes but is not limited to:

Ensuring education regarding safe and responsible use precedes internet access.

Reinforcing online safety messages whenever technology or the internet is in use.

Educating pupils/students in the effective use of the internet to research, including teaching them to be critically aware of the materials they read and how to validate information before accepting its accuracy.

Schools in the Rayleigh Schools Trust recognise that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm. Relevant members of staff, e.g., SENDCo and CIC Co-ordinator, work together so that, where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, which may include but is not limited to those with mental health needs, children in care, victims of abuse and some pupils with SEND.

If a staff member is concerned about anything pupils raise during online safety lessons or activities, or if a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

5.2: Education and engagement of parents/carers

Schools in the Rayleigh Schools Trust recognise that parents/carers have an essential role to play in enabling pupils to become safe and responsible users of the internet and digital technology, and will work in partnership with parents/carers to ensure pupils stay safe online at school and at home. It is noted that many parents/carers, like many adults, have only a limited understanding of online safety risks and issues, and in particular may underestimate how often children and young people come across potentially harmful and inappropriate information on the internet and may be unsure how to respond.

Schools in the Rayleigh Schools Trust wil

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 they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware of and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

Abuse between young people in intimate relationships online.

Preventing and addressing cyber-bullying

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

Schools in the Rayleigh Schools Trust will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. This is included in the safeguarding curriculum covered within tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes CPRE and other subjects where appropriate.

All staff, Governors/Trustees, and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's behaviour and anti-bullying policies.

Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure that the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable groups to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Schools in the Rayleigh Schools Trist are aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

6.2: Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside school and on and offline and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if using systems that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

Threatening, facilitating, or encouraging sexual violence.
Voyeurism and skirting.
Sexualised online bullying.
Unwanted and unsolicited sexual comments and messages.
Consensual or non-consensual sharing of sexualised imagery.
Abuse between young people in intimate relationships online.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to present such behaviour as trivial or harmless. Staff will be aware that allowing such behaviour leads to pupils becoming less likely to report such conduct, and is contrary to the school's culture and ethos.

Staff will be aware that creating, possessing, and distributing indecent imagery of children (i.e., individuals under the age of 18) is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the

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' mental health, both positively and negatively. The DSL will ensure that training is available to help ensure that staff understand popular social media platforms and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Child Protection and Safeguarding and SEND policies.

6.7: Online hoaxes and harmful online challenges

For the purposes of this policy, an 'online hoax' is defined as a deliberate lie designed to seem truthful,

Pose a risk to staff or pupils, and /or

7.1: Filtering and monitoring online activity

Rayleigh Schools Trust will ensure that appropriate filtering systems are in place to prevent staff and pupils/students from accessing unsuitable or illegal content. We will monitor the websites visited by pupils/students, staff, volunteers, Governors and visitors (where relevant) to ensure that they comply with the above.

Our Senso monitoring system and Smoothwall filtering system will:

- Inspect everything that is typed or done on school-owned computers;
- Take screen shots and will report any suspicious use detected on school-owned computers;
- Detect when proxy bypass sites have been used;
- Help to stop downloads of obscene or offensive content;
- Potentially get an early warning of grooming;
- Help warn when pupils/students are planning to meet people they do not know;
- Help pick up cries for help by identifying searches related to suicide, self-harm and abuse.

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.

Users are required to lock access to devices and systems when they are not in use.

Only current pupils, parents/carers and staff will have access to Rayleigh Schools' Trust systems and platforms.

7.3: Emails
Staff and pupils are given school email accounts. Prior to being authorised to use the email system, staff and pupils must agree to the Acceptable Use Agreement. Personal email accounts are not permitted to be used for school, and may be blocked. Equally, pupils/students may only use their school provided email accounts for educational purposes. Any email that contains sensitive or personal information that is being sent outside the organisation should only be sent using secure and/or encrypted methods.

Staff are not permitted to communicate with pupils or parents using personal email accounts.

Staff and pupils are required to report junk/phishing messages to the Network Manager. The school's email system is configured to reduce threats from emails and attachments. Staff and pupils should immediately inform a member of the Leadership Team if they receive an offensive communication.

7.4: Social networking[1]
Personal use
Access to social networking sites is filtered. Staff and pupils are not permitted to use social media for personal use on the school network. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are expected to follow these expectations at all times.

<u>Staff</u>
Staff are strongly advised to safeguard themselves and their privacy on social media. This includes but is not limited to:

- Being aware of location sharing services.
- Setting the privacy levels of their personal sites as strictly as they can.
- Regularly checking the security settings on personal social media profiles to minimise the risk of loss of personal information.
- Opting out of public listings on social media.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Carefully considering the information, including text and images, they share and post online and should ensure that that their social media use is compatible with their professional role, and the wider professional and legal framework. In particula53 Tm0 G[3078]TETQq0.000008866 0 594.96 842.04 reW*nBT/F1

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

Pup

At Sweyne Park School, if pupils/students bring a mobile device into school, it must be switched off and placed in their bag or locker at all times. Where a pupil uses features on a personal device, e.g., to support with managing a medical condition, the arrangements and rules for this are developed and managed on a case-by-case basis.

Further information can be found in Appendix 3 of the Sweyne Park School Behaviour Policy.

At Glebe Primary School, if pupils bring a mobile device into school, it must be given to their teacher who will store it securely for them until the end of the day.

Staff should not use their personal devices during lesson time, other than to request support from another member of staff (e.g., to request a First Aider from Pupil Services or to request the support of a senior member of staff in response to a behaviour incident). Staff are not permitted to use their personal devices to take photos or videos of pupils, nor to store data relating to other staff or pupils/students. They should use only school-

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND

Appendix 3: acceptable use agreement for staff, Governors, Trustees, volunteers and visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, TRUSTEES, VOLUNTEERSNAND VISITORS
Name:

When using the school's ICT systems and accessing the internet in school, or outside school ona work device (if applicable), I will not:

Access, or attempt to access, inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or share such material).
Use them in any way which could harm the reputation of the school or Rayleigh Schools Trust.
Access social networking sites or chat rooms.
Use any improper language when communicating online, including in emails or other messaging services.
Install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
Share my password with others or log in to the school's network using someone else's details.