THE SWEYNE PARK SCHOOL

Online Safety Policy

Prepared in Consultation with:	**Sweyne Park School LGB**
Last reviewed on:	**September 2025**
Approved by Rayleigh Schools Trust:	**December 2025**
Next review by:	**Autumn 2026**

Contents

1: Introduction

Rayleigh Schools Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout our schools; therefore, there are several controls in place to ensure the safety of pupils and staff. Furthermore, the use of the internet and associated devices, are an important part of everyday life. The Rayleigh Schools Trust therefore believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all members of the schools' community (including staff, pupils/students, volunteers, parents/carers, visitors, community users) who have access to and are users of the schools' digital systems, both in and out of the schools.

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, antisemitism, 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, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm such as making, sending or 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 scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. This policy has been created with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils / students, staff, visitors, and other members of the schools' community.

2: Aims

The schools in the Rayleigh School Trust aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and other members of the community.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole community in our schools in their use of technology, including mobile and smart technology (which we generally refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

3: Legislation and guidance

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

- Teaching online safety in schools (DFE, 2019)
- Preventing and tackling bullying (DFE, 2017)
- Cyber-bullying: advice for headteachers and school staff (DFE, 2014)
- Relationships and sex education (DFE, 2021)
- Searching, screening and confiscation (DFE, 2022)
- Filtering and Monitoring Standards for Schools and Colleges (DFE, 2023)
- Generative Artificial Intelligence in Education (DFE, 2023)
- Harmful online challenges and online hoaxes (DFE, 2021)

It also refers to the DFE's guidance on protecting children from radicalisation and UK Council for Internet Safety guidance on Sharing Nudes and semi-nudes.

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 who oversees online safety at Sweyne Park School is **Jennifer Downes**; the Governor who oversees online safety at Glebe Primary School is **Katie Bryan**.

- The online safety Governor will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training and monitor online safety records.

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 incidents in line with the school's child protection and safeguarding policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

- 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 from potentially harmful and inappropriate content and content 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, and that users may only access the school network and school devices through a properly enforced password protection policy.
- To ensure that the DSL (and/or a deputy) has appropriate access to the school's filtering and monitoring systems, to enable them to take appropriate safeguarding action when required.
- Conducting a full security check and monitoring the school's ICT systems on a regular basis in order that any misuse or attempted misuse can be reported to the relevant member of staff for investigation and further action.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

4.5: All staff and volunteers

All staff, including agency staff and contractors, and volunteers are responsible for:

- Ensuring that they have an up-to-date awareness of online safety matters and 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 3), which must be signed and returned.
- Ensuring that pupils/students follow the school's terms on acceptable use (appendices 1 and 2), and that pupils/students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Understanding that technology is a significant component in many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face-to-face. In many cases abuses will take place concurrently via online channels and in daily life. Children can also abuse their peers online: this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of

indecent images, especially around group chats, and the sharing of abusive images to pornography, to those who do not want to receive such content.

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing the Network Manager and DSL without delay.
- Monitoring the use of digital technologies in lessons and other school activities and implement school policies with regard to this. In lessons where internet use is pre-planned pupils/students should be guided to sites checked as suitable for their use.
- Following the correct procedures by speaking with their department or year team SLT line Manager if they need to bypass the filtering and monitoring systems for educational purposes.
- Reporting any online safety incidents on My Concern and/or in person to the DSL, and working with the safeguarding team to ensure that they are dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the 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'.
- Maintaining a professional level of conduct in their personal use of technology.
- Ensuring that all digital communications with pupils/students and their parents/carers are on a professional level and only carried out using school systems.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

This list is not intended to be exhaustive.

4.6: Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Schools in the Rayleigh Schools Trust will take every opportunity to help parents to understand these issues. Parents/carers will be encouraged to support the schools in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images at school events.
- Their child's personal devices in the school.

Parents/carers are expected to:

- Notify a member of staff 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 (appendices 1 and 2).

Parents/carers can seek further guidance on keeping children safe online from the following organisations:

- What are the issues – UK Safer Internet Centre
- Hot topics – Childnet International

4.7: Pupils/Students

Pupils/students are responsible for:

- Adhering to the terms on acceptable use of the school's ICT systems and the internet (appendices 1 and 2).
- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Respecting the feeling and rights of others both on and offline.
- Taking responsibility for keeping themselves and others safe online
- Seeking help from school staff if things go wrong, for example if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns to school staff.

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: Visitors and members of the community

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 3).

5: Education and engagement about online safety

5.1: Education and engagement of pupils

Pupils will be taught about online safety as part of the curriculum. Schools in the Rayleigh Schools Trust refer to the DFE's guidance *Teaching Online Safety in Schools* (DFE, 2019) during the creation of the curriculum. Online safety is embedded within the curriculum and teaching is appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently. The online risks that the pupils may face online are considered when developing the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In **Key Stage 2**, pupils 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**, pupils 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 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 sort 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**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognize inappropriate content, contact and conduct, and how to report concerns.

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 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 training 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, in particular:
    - how the internet can be used to facilitate abuse and exploitation.
    - that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that abuse will frequently take place concurrently on and offline.
- That children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing or indecent nude and semi-nude images and/or videos, especially around group chats.
    - Sharing of abusive images and pornography, to those who do not wish to receive such content.
- Physical abuse, sexual violence and initiation / hazing type violence can all contain an online element.

Training will also help staff:

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

In addition, the DSL and other members of the safeguarding team will provide guidance/advice to individuals as required.

The DSL and DDSLs will undertake Level 3 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.

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

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.

The victim of online sexual behaviour may ask for no-one to be told about the abuse. Confidentiality will not be promised, and the DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately, the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and/or other appropriate staff members will liaise with the victim's parents/carers to discuss the safeguarding measures that are being put in place to support their child and how the report will progress. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully, and appropriate support provided to the victim.

Concerns regarding a pupil's online behaviour are reported using My Concern, and are investigated by the DSL/DDSL in conjunction with relevant staff members (e.g., pastoral staff, ICT technicians), and concerns are managed in accordance with relevant policies depending on their nature, e.g., the Behaviour Policy, the Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the police will be contacted. The DSL will decide in which cases this response is appropriate and will manage such cases in line the with the Child Protection and Safeguarding Policy.

N.B.: Many online safety concerns among children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour. However, some incidents may affect our culture or pose a risk to children and young people's health and wellbeing. Where online behaviour poses a threat or causes harm to other students, or could have an effect on the orderly running of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our Behaviour and/or Child Protection and Safeguarding Policies.

6.1: Cyber-bullying

Definition

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, where the relationship involves an imbalance of power. (See also the schools' behaviour policy.) It can include, but is not limited to, the following:

- Threatening, intimidating, discriminatory or upsetting messages.
- Threatening or embarrassing media sent via electronic means.
- Silent or abusive phone calls or using the victim's device to harass others, to make them think the victim is responsible.
- Unpleasant or defamatory comments/information/messages posted online.

- 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 alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will deal with these incidents in accordance with the behaviour, Anti-bullying, and Child Protection and Safeguarding policies.

6.3: Grooming

Grooming is defined as a situation in which a person builds a relationship, trust and emotional connection with a child with the intention of manipulation, exploitation and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are generally unlikely to report this.

Owing to the fact that pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this kind of abuse. The DSL will ensure that safeguarding training covers online abuse, the importance of looking for signs of grooming and what the signs of grooming are, including but not limited to:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one who does not attend the school and whom their close friends have not met.
- Having money or new possessions that they cannot or will not explain.

6.4: Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g., sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have concerns about pupils with relation to CSE or CCE, they will report this to the DSL and/or by making a report on My Concern and this will be managed in line with the Child Protection and Safeguarding Policy.

6.5: Radicalisation and Extremism

Radicalisation is the process by which a person comes to support terrorism / extremist ideologies. This process can occur through direct recruitment, e.g., individuals in extremist groups identifying, targeting, and contacting young people with the intention of involving them in radical activity or by exposure to extreme ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they are likely to believe that the extremist has their best interests at heart, making them more likely to adopt to same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have concerns about pupils with relation to radicalisation, they will report this to the DSL and/or by making a report on My Concern and this will be managed in line with the Child Protection and Safeguarding Policy.

6.6: Mental Health

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, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, 'harmful online challenges' refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media, and daring others to do the same. Although many online challenges are innocuous, an online challenge become harmful when it could potentially put the participant at risk of harm, either directly as a result of participating in the challenge itself or indirectly as a result of the distribution of the video online.

Where staff suspect that there may be an online hoax or harmful online challenge circulating amongst pupils in the school, they will report this to the DSL (or a deputy) immediately.

The DSL will conduct an assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils.

The DSL and Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasingly pupils' exposure to the risk is considered and mitigated as far as possible.

6.8: Cyber crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled:** these crimes can be carried out offline but are made easier and can be conducted at higher scales and speeds online. Examples include fraud, the purchasing and sale of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent**: These crimes can only be carried out online or using a computer. Examples include making, supplying, or obtaining malware, illegal hacking, and 'booting', which involves overwhelming a computer, network, or website with internet traffic to render it unavailable.

The school is aware of the risk that pupils with a particular affinity or skill in technology may become involved in cyber-crime, whether deliberately or inadvertently.

The schools will ensure that pupils are taught, throughout the curriculum, how to use technology safety, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from the lawful use of the internet, on the school network or school devices through the use of appropriate filtering and monitoring.

6.9: Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (see behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- 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.

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.
- Log all websites visited from any device connected to the internet via the school network.

Concerns identified through monitoring are reported to the DSL using My Concern who manages the report in line with the Child Protection and Safeguarding Policy.

The Rayleigh Schools Trust network uses age-appropriate filtering and the system in place that does not led to unreasonable restrictions on what pupils can be taught. Access levels to the internet are reviewed to reflect the curriculum requirements and the age of the pupils/students.

Leaders are aware of the need to prevent 'over blocking', as that may unreasonably restrict what can be taught. The DSL, in conjunction with the Headteacher and Systems Manager, determine what filtering and monitoring systems are required by the schools. The systems the schools implement are appropriate to the pupils' ages, the number of pupils using the network, and the proportionality of costs compared to the risks. The Systems Manager is responsible for monitoring the filtering and monitoring systems to ensure that they are affective and appropriate.
Change requests for the filtering systems should be directed to the Network Manager and DSL – both need to agree before a change is made.

Rayleigh Schools Trust will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of the internet, it is not possible to guarantee that access to unsuitable material will never occur via a Rayleigh Schools Trust computer or device.

Staff should be aware that they cannot rely on filtering alone to safeguard students/pupils. Prior to the use of any websites, apps, tools, or other online platforms within the school, or recommending that pupils use these platforms at home, the class teacher will always review and evaluate the resource. Equally, supervision of pupils when they are using the internet and education about safe and responsible use is essential.

7.2: Network Security

A layered approach to security is taken at schools in the Rayleigh Schools Trust and it managed by the Systems Manager. Antivirus software is installed and kept up to date. Device firewalls are switched on at all times and application controls are employed to restrict access.

Staff and pupils are not permitted to download/run unapproved software and must remain vigilant to threats from malicious email attachments. Staff and pupils are expected to report any incidents to the Systems Manager.

All members of staff and pupils/students have their own unique usernames and private passwords to access the school's systems. Staff and pupils are responsible for keeping their passwords private. Passwords have a

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.

Staff
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 particular, no reference should be made in social media to students/pupils, parents/carers or staff, and staff should not engage in online discussion on personal matters relating to members of the schools' community.
- Not identifying themselves as employees of Rayleigh Schools Trust or its schools on their personal social media accounts. This is to prevent information on those sites being linked with the Rayleigh Schools Trust and also to safeguard the privacy of staff and the wider schools' community.
- Personal opinions should not be attributed to the school or to Rayleigh Schools Trust.

[1] Social networking includes, but is not limited to: social media apps, blogs, wikis, online gaming, video/photo sharing sites, chatrooms and instant messenger.

- 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; concerns regarding the online conduct of a pupil/student are reported to the DSL through My Concern. These reports will be managed in accordance with the relevant policy.

Use on behalf of the school

The schools' official social media channels are used only for educational or engagement purposes. Staff members must be authorised by the headteacher to access the schools' social media accounts.

7.5: The school website

The Headteacher is responsible for the overall content of the school's website – they will ensure that the content is appropriate, accurate, up-to date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils/students is not published on the website without explicit permission.

7.6: Publishing images and videos online

On entry to the school parents/carers are asked for their consent for the use of images and videos of their children to be taken and used in an educational context, such as in the weekly newsletters and school website.

8: Using mobile devices in school

Any personal electronic device that is brought into school is the responsibility of the owner/user. Rayleigh Schools Trust accepts no responsibility for the loss, theft or damage of such items. Anyone bringing a personal electronic device into school is advised to ensure that they do not contain any content which may be considered offensive, derogatory or would otherwise contravene Rayleigh Schools Trust's policies.

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 2 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-provided equipment for this purpose.

Staff must report concerns about other members of staff use of personal devices on the school premises to the Headteacher.

Information is provided to visitors about the expected use of mobile devices. Any concerns about visitors' use of mobile devices on the school premises should be challenged when safe and appropriate, and reported to the DSL, or any member of the Leadership Team.

9: Staff using work devices outside school

Staff members may be issued with devices (e.g., laptops, mobile phones, or cameras) to assist with their work. Pupils are provided with school-owned devices as necessary to assist with the delivery of the curriculum. School-owned devices are used in accordance with the acceptable use agreements.

The Network Manager monitors school-owned devices and automates the installation of software updates and antivirus definitions. No software, apps or other programmes can be downloaded onto a device without authorisation from the Network Manager.

All staff members 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 a currency symbol).
- Ensuring that their hard drive is encrypted – this means that if the device is lost or stolen, no one can access to 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 by always installing the latest updates

Staff must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 3.

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 the Systems Manager.

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.

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 and staff disciplinary procedures. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content or otherwise serious incidents, should be reported to the police.

11: Monitoring arrangements

This policy will be reviewed at least annually by the DSL – Rayleigh Schools Trust. At every review, the LGB of each school in the Trust will be consulted and asked to recommend for approval by the Board of Trustees. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

12: Links with other policies

This policy links to the following policies and procedures for each of the schools in Rayleigh Schools Trust:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

<table>
<tr><th colspan="2">ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them.
• Only use websites that a teacher or adult has told me or allowed me to use.
• Tell my teacher straight away if:
▪ I click on a website by mistake.
▪ I receive messages from people I don't know.
▪ I find anything that may upset or harm me or my friends.
• Use the school computers for school work only.
• Be kind to others and not upset or be rude about them.
• Look after the school's ICT equipment and tell a teacher straight away if something is broken or not working properly.
• Only use the username and password I have been given.
• Never share my password with anyone, even my friends.
• Never give my personal information (my name, address of telephone numbers) to anyone without the permission of my teacher or parent/carer.
• Save my work on the school network.
• Check with my teacher before I print anything.
• Log off or shut down a computer when I have finished using it.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

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 PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only.
- Only use them when a member of staff is present, or with a member of staff's permission.
- Keep my usernames and passwords safe and not share them with others.
- Keep my private information safe at all times, and not give my name, address, or telephone number to anyone without the permission of a member of staff or my parent/carer.
- Tell a member of staff immediately if I find any maternal which might upset, distress or harm me or others.
- Always log off or shut down a computer when I have finished working on it.

I will not:

- Access or attempt to access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.
- Use any inappropriate language when communicating online, including in emails.
- Create, link to or post any material which is offensive, obscene or otherwise inappropriate.
- Access or attempt to access anyone else's account.
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

- Pupils must not communicate with or attempt to communicate with staff members using social media networks or personal email addresses.
- Pupils must not post or upload any defamatory, objectionable or private material, including images and videos of pupils, staff or parents/carers, to ay website or platform.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

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. • Take photographs of pupils without first checking with a member of staff. • Share confidential information about the school, its pupils or staff, or other members of the community. • Access, modify or share data I am not authorised to access, modify or share. • Promote private businesses, unless that business is directly related to the school. ~ • I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purposes of fulfilling the duties of my role. • I will not use personal email accounts to send or receive data in relation to my role in the school. • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside school, and keep all data securely stored in accordance with the online safety policy and the school's data protection policy. • I will let the Designated Safeguarding Lead (DSL) and Systems Manager know if a pupil/student informs me that they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that the pupils in my care do so too. ~ • I will not use personal mobile devices to take photographs or videos of pupils or staff. • I will not accept or send 'friend' or 'follow' requests from or to pupils or parents/carers on social media. • I will not communicate with pupils or parents/carers on social media or personal email. Contact with pupils or parents will be done through the school's email. (If I have a previously existing relationship that would affect this, this should be discussed with the Headteacher or DSL. • I will not post or upload any defamatory, objectionable, copyright-infringing, or private material, including images or videos of pupils, staff or parents/carers, on any website or other online platform. • I will ensure that I apply appropriate privacy settings to any social media.

~ • 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.

Signed:	**Date:**