

South Shore Academy

E-Safety & ICT Policy



Approved by:	N Kay
Last reviewed on:	1/9/2026
Next Review due by:	1/9/2027

CONTENTS

1. Introduction
2. Legislation and Guidance
3. Roles and Responsibilities
4. Educating Pupils About Online Safety
5. Educating Parents About Online Safety
6. Cyber-Bullying
7. Examining Electronic Devices
8. Filtering and Monitoring
9. Acceptable Use of the Internet in School
10. Email and Communication Systems
11. Social Networking and Personal Publishing
12. Publishing Content and the School Website
13. Publishing Pupil Images and Information
14. Video Conferencing and Webcams
15. Pupils Using Mobile Devices in School
16. Staff Using Work Devices Outside School
17. Youth-Produced Sexual Imagery (Sexting)
18. Data Protection and Personal Information
19. Emerging Technologies
20. How the School Will Respond to Online Safety Issues
21. Training and Awareness
22. Monitoring and Review
23. Links with Other Policies

Appendices:

- Appendix 1: Acceptable Use Agreement – Pupils
- Appendix 2: Acceptable Use Agreement – Staff
- Appendix 3: Acceptable Use Agreement – Parents/Carers
- Appendix 4: Online Safety Incident Report Form

INTRODUCTION

Our Vision for Online Safety

At South Shore Academy, we are committed to fostering an environment of aspiration underpinned by our school values of **Ambition, Purpose & Achievement**. We believe in the power of mutual respect and the importance of honouring one another, both in the physical world and online.

As part of CIDARI Multi-Academy Trust, our mission is to nurture our students' spiritual, moral, cultural, intellectual, and physical development within a caring and supportive community. This includes preparing them to navigate the digital world safely, responsibly, and confidently.

We recognise that technology and the internet are powerful tools that can enhance learning, foster creativity, and open up new opportunities for our pupils. However, we also acknowledge that the online world presents risks that can cause significant harm to children and young people.

This policy sets out our approach to online safety, including:

- How we will protect and educate our pupils about online risks
- How we will support staff to use technology safely and responsibly
- How we will engage parents and carers in keeping children safe online
- How we will respond to online safety incidents

Why Online Safety Matters

The internet and digital technologies are integral to modern life. Our pupils use technology for learning, socialising, entertainment, and increasingly, for their future careers. However, the online world also exposes children and young people to a range of risks, including:

- **Cyberbullying** – being bullied, harassed, or threatened online
- **Online grooming and exploitation** – being targeted by adults or peers for sexual or criminal purposes
- **Exposure to inappropriate content** – including pornography, violence, hate speech, self-harm, and extremist material
- **Youth-produced sexual imagery (sexting)** – creating, sharing, or being pressured to share nude or semi-nude images
- **Online reputation and digital footprint** – the permanence of online activity and its potential impact on future opportunities
- **Privacy and data protection** – sharing personal information that can be misused
- **Misinformation and fake news** – being exposed to false or misleading information
- **Excessive screen time and gaming** – the impact on mental health, sleep, and wellbeing
- **Online radicalisation** – being exposed to extremist views and ideologies
- **Commercial risks** – online gambling, scams, and inappropriate advertising
- **AI-generated content** – including deepfakes, AI-generated sexual imagery, and manipulated media

At South Shore Academy, we take these risks seriously and are committed to providing a safe online environment for all members of our school community.

Our Approach to Online Safety

Our approach to online safety is based on **four key principles**:

1. Education

We believe that education is the most effective way to keep children safe online. We will:

- Teach pupils about online risks and how to protect themselves
- Embed online safety across the curriculum, not just in PSHE or Computing
- Provide regular training for staff to ensure they are equipped to teach and model safe online behaviour
- Engage parents and carers in supporting their children to stay safe online

2. Protection

We will put in place robust systems and procedures to protect pupils from online harm. We will:

- Use appropriate **filtering and monitoring systems** to prevent access to inappropriate content and identify potential safeguarding concerns
- Ensure all staff understand their safeguarding responsibilities in relation to online safety
- Respond swiftly and effectively to online safety incidents
- Work with external agencies (e.g., police, social care, CEOP) where necessary

3. Empowerment

We will empower pupils to take responsibility for their own online safety and to make informed, responsible choices. We will:

- Encourage pupils to report concerns without fear of getting into trouble
- Teach pupils critical thinking skills so they can evaluate online content and recognise risks

- Support pupils to develop a positive digital footprint and online reputation
- Celebrate positive uses of technology

4. Partnership

We recognise that keeping children safe online is a shared responsibility between school, parents, and the wider community. We will:

- Work in partnership with parents and carers to reinforce online safety messages at home
- Engage with external organisations and experts to enhance our online safety provision
- Share best practice with other schools and trusts
- Listen to pupil voice and involve pupils in shaping our online safety approaches

Scope of This Policy

This policy applies to:

- **All pupils** at South Shore Academy
- **All staff**, including teachers, support staff, supply staff, volunteers, and governors
- **All visitors** to the school who use our ICT systems or devices
- **All use of technology and the internet** in school, including:
 - School-owned devices (e.g., computers, laptops, tablets, mobile phones)
 - Personal devices brought into school (e.g., mobile phones, smartwatches)
 - School network and internet connection
 - School email and communication systems
 - Online learning platforms and educational software
 - Social media and messaging apps (where relevant to school activities)

This policy also applies to staff use of school devices and systems **outside of school hours** (e.g., working from home, using school email on personal devices).

LEGISLATION AND GUIDANCE

This policy is based on the following legislation and guidance:

Statutory Guidance and Legislation

- **Keeping Children Safe in Education (KCSIE) 2026** – Statutory safeguarding guidance that includes requirements for online safety (Part 1, paragraphs 139-148; Annex D)
- **Data Protection Act 2018 and UK GDPR** – Legislation governing the processing of personal data
- **Computer Misuse Act 1990** – Legislation criminalising unauthorised access to computer systems
- **Communications Act 2003** – Legislation criminalising sending offensive or menacing messages electronically
- **Malicious Communications Act 1988** – Legislation criminalising sending indecent, grossly offensive, or threatening messages
- **Education Act 2011** – Gives schools the power to search for and delete inappropriate images or files on electronic devices (sections 2 and 3)
- **Equality Act 2010** – Protects people from discrimination, including online harassment based on protected characteristics
- **Public Order Act 1986** – Criminalises stirring up hatred (including online)
- **Protection from Harassment Act 1997** – Protects individuals from harassment, including cyberbullying
- **Sexual Offences Act 2003** – Criminalises sexual offences, including grooming and indecent images of children
- **Serious Crime Act 2015** – Criminalises controlling or coercive behaviour
- **The Prevent Duty (2015)** – Requires schools to prevent pupils from being drawn into terrorism, including online radicalisation

Non-Statutory Guidance

- **DfE guidance: Teaching online safety in schools (2019)** – Non-statutory guidance on teaching online safety
- **UK Council for Internet Safety (UKCIS) guidance: Education for a connected world (2020)** – Framework for teaching online safety from ages 4-18
- **DfE guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people (2020)** – Guidance on responding to youth-produced sexual imagery
- **DfE guidance: Searching, screening and confiscation (2022)** – Guidance on schools' powers to search pupils and confiscate items

Trust and School Policies

This policy reflects **CIDARI Multi-Academy Trust's E-Safety Policy** and operates in conjunction with our:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Staff Code of Conduct
- Mobile Phone Policy (Pupils)
- Social Media Policy
- Complaints Policy

ROLES AND RESPONSIBILITIES

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will:

- Ensure the school has appropriate filtering and monitoring systems in place
- Review this policy annually
- Ensure online safety is a running and interrelated theme throughout the school's safeguarding and child protection policies
- Ensure the school meets its statutory duties under KCSIE 2026 in relation to online safety
- Receive an annual report on online safety from the Headteacher and DSL

The Governing Body will appoint an Online Safety Governor.

The Online Safety Governor will:

- Take the lead on online safety at governing body level
- Meet regularly with the DSL and Online Safety Lead to review online safety provision
- Report to the full Governing Body on online safety matters

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 will:

- Ensure all staff receive appropriate online safety training
- Ensure online safety is embedded in the curriculum
- Ensure parents are informed about online safety
- Work with the DSL to ensure online safety incidents are managed appropriately
- Ensure the school has appropriate filtering and monitoring systems in place
- Report to the Governing Body on online safety matters

The Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- Taking the lead on online safety issues in school
- Supporting staff with online safety concerns
- Managing online safety incidents in line with the school's safeguarding procedures
- Liaising with external agencies (e.g., police, social care, CEOP) where necessary
- Keeping records of online safety incidents on CPOMS
- Ensuring online safety is included in safeguarding training for all staff
- Providing regular updates to the Headteacher and Governing Body on online safety

The DSL at South Shore Academy is:

Danny Mulholland

Deputy DSLs are:

Andrew Monk

Karen Lewis

Sharon Senior

Victoria McCullion

Nicola Miller

The Online Safety Lead

The Online Safety Lead is responsible for:

- Day-to-day management of online safety in school
- Ensuring filtering and monitoring systems are effective
- Delivering online safety training to staff
- Coordinating the online safety curriculum
- Engaging with parents on online safety
- Keeping up to date with emerging online risks and technologies
- Working with the DSL to manage online safety incidents
- Maintaining online safety resources and displays around school

The Online Safety Lead at South Shore Academy is: Danny Mulholland

The IT Network Manager

The IT Network Manager is responsible for:

- Maintaining the school's ICT infrastructure and ensuring it is secure
- Managing filtering and monitoring systems in collaboration with CIDARI MAT IT Team
- Reporting any online safety concerns to the DSL or Online Safety Lead immediately
- Ensuring all users have appropriate access levels
- Ensuring school devices are secure and up to date with security patches
- Managing user accounts and passwords
- Providing technical support for online safety systems

The IT Network Manager at South Shore Academy is: TEL Group

All Staff

All staff are responsible for:

- Reading and following this policy
- Signing the Staff Acceptable Use Agreement annually
- Modelling safe and responsible use of technology
- Teaching pupils about online safety as part of the curriculum
- Reporting any online safety concerns to the DSL **immediately**
- Completing online safety training (as part of safeguarding training)
- Being vigilant to signs that a pupil may be experiencing online harm
- Challenging inappropriate online behaviour (e.g., cyberbullying, sharing inappropriate content)
- Following the school's procedures for using technology (e.g., email, social media, video conferencing)

All staff must understand that:

- Online safety is a safeguarding issue
- They have a duty to report concerns, even if they are unsure
- Failure to report concerns or follow this policy may result in disciplinary action

Parents/Carers

Parents/carers are expected to:

- Support the school's online safety approaches
- Discuss online safety with their children at home
- Monitor their children's use of technology and the internet at home
- Report any concerns to the school
- Follow the school's social media policy (e.g., not posting images of other pupils without permission)
- Sign the Parent/Carer Acceptable Use Agreement
- Attend online safety workshops and events offered by the school

Pupils

Pupils are expected to:

- Read and follow the Pupil Acceptable Use Agreement
- Report any online safety concerns to a trusted adult (teacher, parent, DSL, Anti-Bullying Ambassador)
- Treat others with respect online
- Not share personal information online
- Not create, share, or forward inappropriate content (including nude or semi-nude images)
- Not engage in cyberbullying or online harassment
- Use technology responsibly and in line with school rules

Pupils must understand that:

- The school's online safety rules apply both in school and outside school (where relevant to the school community)
- Breaking the rules may result in sanctions (in line with the Behaviour Policy)
- Some online activities are illegal and may result in police involvement

EDUCATING PUPILS ABOUT ONLINE SAFETY

Our Commitment

At South Shore Academy, we believe that education is the most effective way to keep children safe online. We are committed to ensuring that all pupils receive high-quality online safety education that is:

- **Age-appropriate** – tailored to pupils' developmental stage
- **Relevant** – addresses the risks pupils are actually facing
- **Embedded** – integrated across the curriculum, not just taught in isolation
- **Progressive** – builds on prior learning and develops pupils' understanding over time
- **Empowering** – gives pupils the knowledge and skills to protect themselves

What We Teach

Our online safety curriculum is based on the **UK Council for Internet Safety (UKCIS) framework: Education for a Connected World**, which covers eight key areas:

1. **Self-image and identity** – understanding how online identity can differ from offline identity
2. **Online relationships** – understanding how to build healthy relationships online
3. **Online reputation** – understanding the permanence of online activity and its impact
4. **Online bullying** – understanding what cyberbullying is and how to respond
5. **Managing online information** – understanding how to evaluate online content critically
6. **Health, wellbeing and lifestyle** – understanding the impact of technology on physical and mental health
7. **Privacy and security** – understanding how to protect personal information and stay secure online
8. **Copyright and ownership** – understanding intellectual property and how to use content responsibly

Online Safety Curriculum by Key Stage

Key Stage 3 (Years 7–9)

Pupils will be taught:

Online risks and harm:

- The different types of online risks (cyberbullying, grooming, inappropriate content, etc.)
- How to recognise when they or others are at risk online
- How to report concerns (in school and externally, e.g., CEOP, Childline)

Personal information and privacy:

- What personal information is and why it should be protected
- How to use privacy settings on social media and apps
- The risks of sharing personal information (e.g., identity theft, grooming)

Online relationships:

- The characteristics of healthy and unhealthy online relationships
- How to recognise and respond to online grooming and exploitation
- The importance of consent in online relationships
- How to block and report users who make them feel uncomfortable

Online reputation and digital footprint:

- The concept of a "digital footprint" and its permanence
- How online activity can impact future opportunities (e.g., jobs, university)
- How to manage their online reputation positively

Critical thinking and misinformation:

- How to evaluate the reliability of online information
- How to recognise fake news, clickbait, and misleading content
- The importance of checking sources before sharing information

Cyberbullying:

- What cyberbullying is and how it differs from other forms of bullying
- The impact of cyberbullying on victims
- How to respond if they or someone they know is being cyberbullied
- The role of bystanders in preventing and stopping cyberbullying

Online communication:

- How to communicate respectfully online
- The risks of misunderstanding tone and context in online communication
- The permanence of online messages (e.g., screenshots)

The law:

- The legal implications of online activity, including:
 - Sending indecent images of children (even of themselves)
 - Harassment and threatening behaviour
 - Hate speech and discrimination
 - Copyright infringement

Key Stage 4 (Years 10–11)

Pupils will be taught all of the above, plus:

Youth-produced sexual imagery (sexting):

- The legal, social, and emotional consequences of creating, sharing, or possessing nude or semi-nude images
- How to respond if they receive such images (do not share, report immediately)
- The risks of being pressured to send images

Online grooming and exploitation:

- How groomers operate online (building trust, isolating victims, normalising sexual behaviour)
- The signs of grooming (in themselves and others)
- How to report concerns to CEOP

Social media and mental health:

- The impact of social media on self-esteem, body image, and mental health
- How to recognise when social media use is becoming unhealthy
- Strategies for managing screen time and taking breaks from social media

Online gambling and gaming:

- The risks of online gambling (including in-game purchases and loot boxes)
- How to recognise signs of gambling addiction
- The risks of online gaming (e.g., grooming, exposure to inappropriate content, excessive screen time)

Online radicalisation:

- How extremist groups use the internet to recruit young people
- The signs of radicalisation
- How to report concerns (to school or through the Prevent referral process)

AI and emerging technologies:

- The risks of AI-generated content (e.g., deepfakes, AI-generated sexual imagery)
- How to recognise manipulated media
- The ethical implications of AI

Preparing for adulthood:

- How to use social media and the internet professionally (e.g., for job applications, networking)
- How to protect their online reputation as they transition to further education or employment

How We Teach Online Safety

Online safety is taught through:

PSHE Lessons

- Dedicated online safety lessons each term
- Delivered by Form Tutors with support from the PSHE Lead and Online Safety Lead

Computing Lessons

- Technical aspects of online safety (e.g., passwords, privacy settings, malware, phishing)
- Delivered by Computing teachers

Morning Meetings

- Regular reminders and updates on online safety
- "Online Safety Tip of the Week"
- Responses to emerging risks or incidents

Assemblies

- Themed assemblies on online safety topics (e.g., Anti-Bullying Week, Safer Internet Day)
- Guest speakers from external organisations (e.g., CEOP, Internet Matters, NSPCC)

Cross-Curricular

- Online safety is embedded across subjects where relevant:
 - **English:** Fake news, media literacy, online communication
 - **Science:** Evaluating online sources, misinformation
 - **History/Geography:** Propaganda, online radicalisation
 - **Art/Media:** Copyright, digital citizenship
 - **RE/PSHE:** Respectful online communication, online relationships

Targeted Interventions

- For pupils identified as being at higher risk (e.g., pupils with SEND, looked-after children, pupils involved in online safety incidents)
- Delivered by the Pastoral Team, Engagement Coaches, or external agencies

External Support

We work with external organisations to enhance our online safety education, including:

- **CEOP (Child Exploitation and Online Protection Centre)** – Thinkuknow resources and presentations
- **Internet Matters** – Age-specific online safety advice
- **UK Safer Internet Centre** – Safer Internet Day resources
- **NSPCC** – Online safety resources and workshops
- **Childnet** – Online safety resources and training

Pupil Voice

We actively involve pupils in shaping our online safety provision through:

- **Anti-Bullying Ambassadors** – trained pupils who promote online safety and support peers
- **School Council** – regular discussions about online safety issues
- **Surveys and questionnaires** – gathering pupil views on online safety
- **Focus groups** – consulting pupils on emerging risks and new technologies

EDUCATING PARENTS ABOUT ONLINE SAFETY

Our Commitment

We recognise that parents and carers play a crucial role in keeping children safe online. We are committed to working in partnership with parents to:

- Raise awareness of online risks
- Provide practical advice on how to keep children safe at home
- Reinforce the online safety messages taught in school

How We Engage Parents

We engage parents through:

Information on the School Website

- This policy is published on our website
- Online safety tips and resources for parents
- Links to external organisations (e.g., Internet Matters, NSPCC, UK Safer Internet Centre)

Parent Workshops and Events

- Annual online safety workshop for parents (e.g., during Safer Internet Day)
- Year 7 transition evening (includes online safety information)
- Year 9 options evening (includes online safety and GCSE options)
- Year 11 parents' evening (includes information about online safety and post-16 transitions)

Newsletters and Communications

- Regular updates on online safety in school newsletters
- Alerts about emerging risks (e.g., new apps, online trends, scams)
- Tips for managing screen time and monitoring children's online activity

Parent/Carer Acceptable Use Agreement

- Parents are asked to sign an Acceptable Use Agreement (Appendix 3) which includes:
 - Supporting the school's online safety approaches
 - Monitoring their children's use of technology at home
 - Following the school's social media policy

One-to-One Support

- Parents can contact the DSL or Online Safety Lead for advice on specific concerns
- The Pastoral Team can provide targeted support for families

What We Ask Parents to Do

We ask parents to:

- **Talk to their children** about online safety regularly
- **Set boundaries** around screen time and device use at home
- **Use parental controls** on devices and internet connections
- **Monitor their children's online activity** (e.g., check social media accounts, know their passwords)
- **Be aware of the apps and games** their children are using
- **Model safe and responsible use** of technology
- **Report concerns** to the school if they are worried about their child's online activity
- **Support the school's rules** (e.g., mobile phone policy, social media policy)

Useful Resources for Parents

We recommend the following resources for parents:

- **Internet Matters:** www.internetmatters.org – Age-specific advice and parental controls guides
- **NSPCC Online Safety:** www.nspcc.org.uk/keeping-children-safe/online-safety – Advice on keeping children safe online
- **UK Safer Internet Centre:** www.saferinternet.org.uk – Resources for parents and carers
- **Childnet:** www.childnet.com – Online safety resources and advice
- **Think U Know:** www.thinkuknow.co.uk/parents – Resources from CEOP
- **National Cyber Security Centre:** www.ncsc.gov.uk/cyberaware – Advice on staying secure online
- **Net Aware:** www.net-aware.org.uk – Social media guides for parents (from NSPCC and O2)

CYBER-BULLYING

Definition

Cyber-bullying is bullying that takes place online or through digital devices. It can include:

- Sending threatening, abusive, or hurtful messages (via text, email, social media, gaming platforms)
- Posting or sharing embarrassing, humiliating, or private information about someone
- Creating fake profiles or accounts to impersonate or humiliate someone
- Excluding someone from online groups or activities
- Spreading rumours or gossip online
- Sharing or threatening to share nude or semi-nude images (see Section 17)
- Using AI to create fake or manipulated images or videos of someone (deepfakes)

Cyber-bullying can be particularly harmful because:

- It can happen 24/7
- It can reach a wide audience very quickly
- It can be anonymous (making it harder to identify the perpetrator)
- Evidence can be saved and shared repeatedly
- It can be difficult to escape (as it follows victims into their homes)

Our Approach

South Shore Academy takes cyber-bullying extremely seriously. All incidents of cyber-bullying are treated as **child-on-child abuse** and are managed in line with our **Anti-Bullying Policy** and **Safeguarding and Child Protection Policy**.

We will:

- Respond swiftly to all reports of cyber-bullying
- Support victims and help them feel safe
- Take appropriate action with perpetrators (which may include education, sanctions, or referral to external agencies)
- Work with parents/carers of both victims and perpetrators
- Educate pupils about cyber-bullying and how to prevent it

How to Report Cyber-Bullying

Pupils who are being cyber-bullied, or who witness cyber-bullying, should:

- **Tell a trusted adult immediately** (teacher, parent, DSL, Anti-Bullying Ambassador)
- **Save evidence** (take screenshots, save messages) – but do not share it with others
- **Do not respond** to the bully or retaliate
- **Block the person** if possible (on social media, messaging apps, gaming platforms)

Parents who become aware of cyber-bullying should:

- **Contact the school immediately** (DSL, Form Tutor, Pastoral Team)
- **Save evidence** (take screenshots, save messages)
- **Support their child** and reassure them that it's not their fault

How the School Will Respond

All incidents of cyber-bullying will be:

- **Recorded on CPOMS** with details of the incident and action taken
- **Investigated** by the Pastoral Team or DSL
- **Assessed** to determine the level of risk and appropriate response

Possible responses include:

- **Support for the victim** (counselling, safety planning, monitoring)
- **Education for the perpetrator** (about the impact of their actions and how to make amends)
- **Sanctions** (in line with the Behaviour Policy, which may include detention, isolation, or exclusion)
- **Restorative Justice** (where appropriate and agreed by all parties)
- **Parental involvement** (meetings with parents of both victim and perpetrator)
- **Referral to external agencies** (police, social care, CEOP) where the behaviour is illegal or poses a serious safeguarding risk

For more information, see our Anti-Bullying Policy.

EXAMINING ELECTRONIC DEVICES

Legal Powers

Under the **Education Act 2011** (sections 2 and 3), schools have the power to:

- **Search pupils' electronic devices** (e.g., mobile phones, tablets, smartwatches) if there is reasonable suspicion that the device contains evidence of:
 - A criminal offence
 - A breach of school rules
 - Content that could cause harm to the pupil or others
- **Delete inappropriate images or files** from pupils' devices, including:
 - Pornographic images
 - Nude or semi-nude images of children (including youth-produced sexual imagery)
 - Abusive or threatening messages
 - Evidence of cyberbullying

This power applies to:

- School-owned devices
- Pupils' personal devices (brought into school or used on school premises)

When We Will Search Devices

We will search a pupil's device if we have reasonable grounds to suspect that it contains:

- Nude or semi-nude images of children (including youth-produced sexual imagery)
- Evidence of cyberbullying or online harassment
- Evidence of criminal activity (e.g., threats, hate speech, drug dealing)
- Inappropriate or harmful content (e.g., pornography, violence, self-harm)
- Evidence of radicalisation or extremist content

How We Will Conduct Searches

Searches will be conducted in line with the **DfE guidance: Searching, screening and confiscation (2022)**.

Procedures:

- Searches will be conducted by the Headteacher, a member of the Senior Leadership Team, or a member of staff authorised by the Headteacher
- Searches will be conducted in the presence of another member of staff (as a witness)
- Where possible, the pupil will be asked to unlock the device and show the content voluntarily
- If the pupil refuses, the device may be confiscated and examined by a member of staff
- Parents will be informed if a search is conducted

Safeguarding concerns:

- If the search reveals content that is a safeguarding concern (e.g., nude images, evidence of abuse), the DSL will be informed immediately
- The device may be confiscated as evidence
- The incident will be recorded on CPOMS
- External agencies (e.g., police, social care) may be involved

Deletion of content:

- If inappropriate content is found, it will be deleted unless it is evidence of a criminal offence (in which case it will be preserved for the police)
- Parents will be informed if content has been deleted

Confiscation of Devices

Devices may be confiscated if:

- A pupil is using a device in breach of school rules (e.g., during lessons, in corridors)
- A pupil refuses to unlock a device when asked
- A device contains inappropriate content

Confiscated devices will be:

- Stored securely in the school office

- Returned to the pupil at the end of the day (or to parents, depending on the circumstances)
- Returned to parents if the confiscation is for a longer period (e.g., repeated breaches of the mobile phone policy)

FILTERING AND MONITORING

Our Commitment

South Shore Academy is committed to providing a safe online environment for all pupils and staff. We use **filtering and monitoring systems** to:

- Prevent access to inappropriate content
- Identify potential safeguarding concerns
- Support pupils to make safe choices online

Our systems are designed to be "appropriate" as required by KCSIE 2026, which means they:

- Block access to illegal content (e.g., child sexual abuse material, terrorism)
- Block access to harmful content (e.g., pornography, violence, self-harm, hate speech)
- Identify concerning online behaviour (e.g., searches for self-harm, suicide, radicalisation)
- Are regularly reviewed and updated to reflect emerging risks

Filtering

What We Use

South Shore Academy uses **Smoothwall** to filter internet content and prevent pupils and staff from accessing inappropriate material.

The filtering system is managed by:

- **CIDARI MAT IT Team**
- **IT Network Manager:** TEL Group
- **Online Safety Lead:** Danny Mulholland

What We Block

The filtering system blocks access to:

- **Illegal content:**
 - Child sexual abuse material (CSAM)
 - Terrorism and extremist content
 - Content that incites violence or hatred
- **Harmful content:**
 - Pornography and sexually explicit material
 - Violence and graphic content
 - Self-harm and suicide content
 - Eating disorder content
 - Hate speech and discrimination
 - Drug and alcohol abuse content
- **Security risks:**
 - Malware and phishing sites
 - Hacking and proxy sites
 - Sites that could compromise network security
- **Age-inappropriate content:**
 - Social media sites (where appropriate)
 - Gaming sites (where appropriate)
 - Online gambling sites

Differentiated Filtering

We use differentiated filtering to ensure that:

- **Pupils** have age-appropriate access to the internet
- **Staff** have access to content they need for teaching and professional purposes
- **Sixth form students** (if applicable in future) have more freedom while still being protected

Overblocking

We recognise that filtering systems can sometimes block legitimate educational content ("overblocking").

If staff or pupils find that a website has been blocked inappropriately, they should:

1. Report it to the IT Network Manager or Online Safety Lead
2. Provide details of the website and why it's needed
3. The IT Network Manager will review the request and adjust the filtering settings if appropriate (usually within 24 hours)

Staff should never:

- Use personal devices or mobile data to bypass the school's filtering system
- Share their login credentials with pupils to allow them to access blocked content
- Disable or attempt to bypass the filtering system

Monitoring

What We Use

South Shore Academy uses **Smoothwall Monitor** to monitor internet use and identify potential safeguarding concerns.

The monitoring system is managed by:

- **IT Network Manager:** TEL Group
- **DSL & Online Safety Lead:** Danny Mulholland

What We Monitor

The monitoring system alerts staff to:

- **Searches or visits to concerning websites** (e.g., self-harm, suicide, eating disorders, extremism, pornography)
- **Use of concerning keywords** in searches, emails, or documents (e.g., suicide, self-harm, weapons, radicalisation, sexual content)
- **Attempts to bypass filtering systems** (e.g., using proxy sites, VPNs)

- **Unusual patterns of behaviour** (e.g., accessing the internet at unusual times, repeated attempts to access blocked content)

How Alerts Are Managed

All alerts are treated as potential safeguarding concerns and are responded to promptly:

- **Alerts are reviewed by the DSL or Online Safety Lead** (usually within 24 hours, or immediately for high-priority alerts)
- **The DSL assesses the level of risk** and determines the appropriate response
- **Action is taken**, which may include:
 - Speaking to the pupil to understand the context
 - Providing support or education
 - Recording the incident on CPOMS
 - Informing parents
 - Referring to external agencies (e.g., CAMHS, social care, police, Prevent)
- **The incident is recorded** and monitored

High-priority alerts (e.g., immediate risk of harm, illegal activity) are escalated immediately to the DSL and Headteacher.

Staff and Pupil Privacy

We recognise that monitoring systems can raise concerns about privacy. We are committed to:

- **Being transparent** about what we monitor and why
- **Using monitoring data only for safeguarding purposes** (not for performance management or disciplinary action, unless there is a serious breach of policy)
- **Storing monitoring data securely** in line with the Data Protection Act 2018 and UK GDPR
- **Reviewing monitoring systems regularly** to ensure they are proportionate and necessary

Staff and pupils should be aware that:

- All use of school devices and the school network is monitored
- There is no expectation of privacy when using school systems
- Monitoring is in place to keep everyone safe, not to "spy" on them

Review of Filtering and Monitoring Systems

The filtering and monitoring systems are reviewed **at least once every academic year** by the **Senior Leadership Team, DSL, Online Safety Lead, and IT Network Manager**.

The review considers:

- Whether the systems are blocking/monitoring appropriate content
- Whether there have been any incidents of pupils or staff accessing inappropriate content
- Whether the systems are causing overblocking or generating false alerts
- Whether the systems are fit for purpose given emerging technologies and risks
- Feedback from staff, pupils, and parents

The review is reported to the Governing Body annually, including:

- Number and types of alerts generated
- Number and types of incidents identified
- Action taken in response to incidents
- Any changes made to filtering or monitoring settings
- Recommendations for improvement

ACCEPTABLE USE OF THE INTERNET IN SCHOOL

overview

All users of the school's ICT systems and internet connection are expected to use them **responsibly, safely, and legally**.

This section sets out the rules for acceptable use. More detailed Acceptable Use Agreements for pupils, staff, and parents can be found in Appendices 1–3.

Acceptable Use – Pupils

Pupils are expected to:

DO:

- Use school devices and the internet for **educational purposes only** (unless given permission for other uses, e.g., during break times)
- **Respect others** online – treat people the way you would want to be treated
- **Protect your personal information** – do not share your full name, address, phone number, school name, or other identifying information online
- **Use strong passwords** and keep them private
- **Log out** of devices when you've finished using them
- **Report concerns** immediately to a trusted adult if you see or experience anything online that makes you feel uncomfortable, worried, or unsafe
- **Ask for help** if you're unsure whether something is safe or appropriate

DO NOT:

- Access, create, store, or share **inappropriate content** (including pornography, violence, hate speech, self-harm content)
- **Cyberbully** or harass others online
- **Share or forward** nude or semi-nude images (even if they are of yourself)
- **Pretend to be someone else** online (impersonation)
- **Share your password** with anyone (except your parents)
- **Attempt to bypass** the school's filtering or monitoring systems (e.g., using proxy sites, VPNs)
- **Download or install** software, apps, or files without permission
- **Use the internet for illegal activities** (e.g., hacking, piracy, threats)

- **Share school login details** with anyone outside school

Consequences:

- Breaking these rules may result in sanctions in line with the **Behaviour Policy**, including detention, isolation, or exclusion
- Serious breaches (e.g., sharing indecent images, making threats) may result in police involvement

For full details, see the Pupil Acceptable Use Agreement (Appendix 1).

Acceptable Use – Staff

Staff are expected to:

DO:

- Use school devices and the internet **professionally and responsibly**
- **Model safe and responsible use** of technology to pupils
- **Protect pupil data** and follow the school's Data Protection Policy
- **Use strong passwords** and keep them private
- **Log out** of devices when not in use
- **Report concerns** immediately to the DSL if you see or suspect online harm to a pupil
- **Follow the school's social media policy** (see Section 11)
- **Ensure all online communication with pupils is professional** and takes place through official school channels (e.g., school email, Google Classroom)

DO NOT:

- Access, create, store, or share **inappropriate content** (including pornography, violence, hate speech)
- **Use school devices for personal use** (except where explicitly permitted, e.g., checking personal email during breaks)
- **Share your password** with anyone (including colleagues or pupils)
- **Attempt to bypass** the school's filtering or monitoring systems
- **Download or install** software, apps, or files without permission from the IT Network Manager
- **Use personal devices** to communicate with pupils (e.g., personal mobile phone, personal email, personal social media)

- **Add pupils as "friends" or "followers"** on personal social media accounts
- **Share personal contact details** with pupils or parents (use school contact details only)
- **Take or share images of pupils** without following the school's procedures (see Section 13)

Consequences:

- Breaking these rules may result in disciplinary action, up to and including dismissal
- Serious breaches (e.g., accessing indecent images, grooming) will be reported to the police and may result in referral to the Disclosure and Barring Service (DBS) and Teaching Regulation Agency (TRA)

For full details, see the Staff Acceptable Use Agreement (Appendix 2) and Staff Code of Conduct.

EMAIL AND COMMUNICATION SYSTEMS

School Email Accounts

All staff and pupils have school email accounts provided by **Google Workspace**.

Staff and pupils must:

- Use school email accounts for all school-related communication
- Check their school email regularly
- Use professional and respectful language in all emails
- Not share their email password with anyone

Staff and pupils must not:

- Use school email for personal purposes (except in emergencies)
- Send or forward inappropriate content (including jokes, chain emails, spam)
- Open attachments or click links from unknown senders (report suspicious emails to the IT Network Manager)

Staff Communication with Pupils

All communication between staff and pupils must:

- Take place through official school channels (school email, Google Classroom, school messaging systems)
- Be professional and transparent
- Be appropriate and necessary for educational purposes

Staff must not:

- Communicate with pupils via personal email, personal mobile phone, or personal social media
- Share personal contact details with pupils
- Engage in personal or inappropriate conversations with pupils online

If a pupil contacts a member of staff via personal channels (e.g., personal social media, personal phone), the member of staff must:

- Not respond via personal channels
- Redirect the pupil to official school channels
- Report the incident to the DSL

Staff Communication with Parents

Staff should:

- Communicate with parents via school email or the school's official communication systems (e.g., ClassCharts, ParentPay)
- Maintain professional boundaries in all communication
- Be mindful of working hours (staff are not expected to respond to emails outside of working hours)

Staff should not:

- Share personal contact details with parents
- Communicate with parents via personal social media or personal messaging apps

SOCIAL NETWORKING AND PERSONAL PUBLISHING

Social Media – General Principles

Social media can be a powerful tool for communication, engagement, and learning. However, it also presents risks, particularly in relation to safeguarding, professional boundaries, and reputation.

This section sets out our expectations for staff, pupils, and parents in relation to social media.

School Use of Social Media

South Shore Academy uses social media to:

- Share news and celebrate achievements
- Engage with parents and the wider community
- Promote the school

Official school social media accounts include:

- Twitter/X:
- Facebook:
- Instagram: [Insert handle]

Official school social media accounts are managed by:

- Mrs V Danson, Deputy Headteacher

All posts on official school social media accounts must:

- Be approved by the Headteacher or a member of the Senior Leadership Team
- Be professional and appropriate
- Follow the school's safeguarding procedures (e.g., not identifying pupils by name without parental consent)
- Comply with the Data Protection Act 2018 and UK GDPR

Staff Personal Use of Social Media

Staff are entitled to a private life and to use social media in their personal capacity.

However, staff must:

- Maintain professional boundaries and not bring the school into disrepute
- Set privacy settings on personal social media accounts to "private" or "friends only"
- Not accept friend requests or follow pupils or recent former pupils (within the last 5 years) on personal social media accounts
- Not accept friend requests or follow parents of current pupils on personal social media accounts (unless they have a pre-existing personal relationship)
- Not post anything about the school, pupils, parents, or colleagues that could be considered unprofessional, defamatory, or bring the school into disrepute
- Not share images of pupils taken at school or school events on personal social media accounts
- Be aware that even "private" posts can be shared or screenshot

If staff become aware of inappropriate content about the school, pupils, or colleagues on social media, they should:

- Take a screenshot as evidence
- Report it to the Headteacher or DSL immediately
- Not engage with or respond to the content

Breaches of this policy may result in disciplinary action, up to and including dismissal.

For more information, see our Social Media Policy and Staff Code of Conduct.

Pupils' Use of Social Media

Pupils are not permitted to access social media on school devices or the school network (except where explicitly permitted for educational purposes, e.g., as part of a lesson).

However, we recognise that many pupils use social media outside of school. We educate pupils about:

- The risks of social media (cyberbullying, grooming, privacy, reputation)
- How to use social media safely and responsibly
- How to report concerns

Pupils must:

- Not post anything about the school, staff, or other pupils that could be considered bullying, defamatory, or bring the school into disrepute
- Not share images of other pupils without their permission
- Not impersonate staff or other pupils online
- Report any concerns about social media to a trusted adult

If pupils misuse social media in a way that affects the school community (e.g., cyberbullying, posting inappropriate content about the school), the school may:

- Investigate the incident
- Take disciplinary action in line with the Behaviour Policy
- Involve parents
- Involve external agencies (e.g., police, social care) if the behaviour is illegal or poses a safeguarding risk

The school's Behaviour Policy applies to pupils' conduct outside of school where it:

- Could have repercussions for the orderly running of the school
- Poses a threat to another pupil or member of the public
- Could adversely affect the reputation of the school

Parents' Use of Social Media**We ask parents to:**

- Support the school's online safety approaches
- Not post negative, defamatory, or abusive comments about the school, staff, or other pupils on social media
- Not share images of other pupils on social media without permission from their parents
- Raise any concerns directly with the school (rather than posting on social media)

If parents have concerns about the school, we encourage them to:

- Contact the school directly (via the school office, Form Tutor, or Headteacher)
- Follow the school's Complaints Policy if they are not satisfied with the response

If parents post inappropriate content about the school on social media, the school may:

- Contact the parent to discuss the issue

- Request that the content is removed
- Report the content to the social media platform
- Take legal action if the content is defamatory or poses a safeguarding risk

PUBLISHING CONTENT AND THE SCHOOL WEBSITE

School Website

The school website is managed by **TEL Group**

All content published on the school website must:

- Be approved by the Headteacher or a member of the Senior Leadership Team
- Be accurate and up to date
- Comply with safeguarding requirements (e.g., not identifying pupils by name without parental consent)
- Comply with the Data Protection Act 2018 and UK GDPR
- Be accessible (in line with the Public Sector Bodies Accessibility Regulations 2018)

The school website includes:

- Information about the school (e.g., vision, values, curriculum)
- Policies (including this policy)
- News and events
- Contact information

Publishing Pupil Work

Pupils' work may be published on the school website, social media, or in school displays to celebrate achievements.

When publishing pupil work, we will:

- Seek parental consent (via the annual consent form)
- Only use first names (not full names)
- Not include any personal information (e.g., address, date of birth)
- Ensure the work is appropriate and of a high standard

Pupils will be taught:

- To be proud of their work
- That their work may be shared publicly
- To think carefully about what they create and share online

PUBLISHING PUPIL IMAGES AND INFORMATION

Taking and Using Images of Pupils

We may take and use images of pupils for:

- Celebrating achievements (e.g., on the school website, social media, newsletters)
- Educational purposes (e.g., recording lessons, school events)
- Publicity (e.g., prospectus, marketing materials)

We will always:

- Seek parental consent before taking or using images of pupils (via the annual consent form)
- Only use images that are appropriate and in the best interests of the pupil
- Store images securely in line with the Data Protection Act 2018 and UK GDPR
- Not identify pupils by full name alongside their image (unless we have explicit consent)
- Not include any personal information (e.g., address, date of birth) alongside images

Parental Consent

- Parents are asked to give consent for the school to take and use images of their child via the **annual consent form** (completed at the start of each academic year).

Parents can:

- Withdraw consent at any time by contacting the school office
- Request that images of their child are removed from the school website or social media

If parents do not give consent, we will:

- Not take or use images of their child
- Take reasonable steps to ensure their child is not included in group photos (e.g., by seating them at the edge of the group)

Use of Images by Parents and Visitors

Parents and visitors are welcome to take photos and videos at school events (e.g., sports day, concerts, performances) for personal use.

However, we ask that parents and visitors:

- Do not share images of other pupils on social media without permission from their parents
- Do not take images in changing rooms or toilets
- Do not take images that could embarrass or upset pupils
- Follow the instructions of staff (e.g., if staff ask parents not to take images during a particular part of an event)

If parents or visitors misuse images (e.g., by posting inappropriate images on social media), the school may:

- Contact the parent or visitor to discuss the issue
- Request that the images are removed
- Report the matter to the police if the images pose a safeguarding risk

Use of Images by Pupils

Pupils are not permitted to take images of other pupils or staff on school premises (except where explicitly permitted, e.g., as part of a lesson or school event).

This includes:

- Taking photos or videos on mobile phones, tablets, or cameras
- Taking screenshots of video calls or online lessons

If pupils take inappropriate images (e.g., in changing rooms, toilets, or of a sexual nature), this will be treated as a serious safeguarding concern and may result in:

- Disciplinary action (in line with the Behaviour Policy)
- Confiscation of the device
- Police involvement (if the images are illegal, e.g., indecent images of children)

VIDEO CONFERENCING AND WEBCAMS

Use of Video Conferencing

Video conferencing may be used for:

- Remote learning (e.g., during school closures, for pupils who are isolating)
- Meetings with parents (e.g., parents' evenings, SEND reviews)
- Meetings with external agencies (e.g., educational psychologists, social workers)
- Staff meetings and training

Platforms we use include:

- Google Meet
- Microsoft Teams
- Zoom

Safeguarding During Video Conferencing

When using video conferencing with pupils, staff must:

- Use official school platforms only (not personal accounts)
- Ensure the video call is scheduled and recorded (where appropriate) via the school system
- Ensure another member of staff is present or aware of the call (where possible)
- Ensure the call takes place during school hours (unless there are exceptional circumstances)
- Ensure pupils are appropriately dressed and in an appropriate location (not in bedrooms or bathrooms)
- Ensure the background is appropriate (use virtual backgrounds if necessary)
- Mute pupils when they are not speaking (to avoid background noise or inappropriate comments)
- End the call immediately if there are any safeguarding concerns and report to the DSL

Pupils must:

- Join video calls from a communal area of their home (not bedrooms or bathrooms) where possible
- Be appropriately dressed

- Mute their microphone when not speaking
- Not record, screenshot, or share images from the video call
- Behave appropriately and follow the school's Behaviour Policy

Parents should:

- Ensure their child is supervised during video calls (particularly younger pupils)
- Ensure the environment is appropriate (quiet, well-lit, appropriate background)
- Not join the video call or speak on behalf of their child (unless invited to do so by the teacher)

Use of Webcams

Webcams on school devices must:

- Be covered when not in use (using a webcam cover or tape)
- Only be used for authorised purposes (e.g., video conferencing, recording lessons)
- Not be used to record pupils without their knowledge or consent

Pupils must not:

- Use webcams to record other pupils or staff without permission
- Share recordings or images from webcams on social media or other platforms

PUPILS USING MOBILE DEVICES IN SCHOOL

15.1 Mobile Phone Policy

South Shore Academy has a **no mobile phones during the school day** policy.

Full details can be found in our Mobile Phone Policy.

In summary:

- Pupils **must not use mobile phones during the school day**
- Mobile phones must be **switched off and kept in bags**
- Pupils who breach the mobile phone policy will face sanctions in line with the Behaviour Policy

Smartwatches and Other Wearable Technology

Smartwatches and other wearable technology (e.g., fitness trackers) are not permitted.

Use of Personal Devices for Learning

In some circumstances, pupils may be permitted to use personal devices (e.g., tablets, laptops) for learning.

This will only be permitted where:

- The pupil has been given explicit permission by a member of staff
- The device is used for educational purposes only
- The device is connected to the school's filtered network (not mobile data)
- The pupil follows the school's Acceptable Use Policy

STAFF USING WORK DEVICES OUTSIDE SCHOOL

Use of School Devices at Home

Staff may use school devices (e.g., laptops, tablets) at home for work purposes.

When using school devices at home, staff must:

- Keep the device secure (e.g., locked in a car boot if left in a vehicle, not left unattended in public places)
- Use strong passwords and lock the device when not in use
- Not allow family members (including children) to use the device
- Connect to a secure internet connection (not public Wi-Fi)
- Report any loss, theft, or damage to the IT Network Manager immediately
- Follow the school's Data Protection Policy (e.g., not storing pupil data on personal devices or cloud storage)

Use of Personal Devices for Work

Staff should not use personal devices (e.g., personal laptops, tablets, mobile phones) for work purposes, except in emergencies.

If staff need to use a personal device for work, they must:

- Seek permission from the Headteacher or IT Network Manager
- Ensure the device is secure (password-protected, up to date with security patches)
- Not store pupil data on the device
- Delete any work-related data from the device as soon as possible

Staff must not:

- Use personal email accounts to communicate with pupils or parents
- Store pupil data on personal cloud storage (e.g., personal Google Drive, Dropbox)
- Use personal social media accounts for work purposes

Remote Working

When working remotely (e.g., from home), staff must:

- Use school devices and official school systems (e.g., school email, Google Workspace)
- Connect to a secure internet connection
- Ensure their workspace is private and secure (e.g., not working in public places where screens can be viewed by others)
- Follow the school's Data Protection Policy
- Be contactable during working hours (via school email or phone)

YOUTH-PRODUCED SEXUAL IMAGERY (SEXTING)

Definition

Youth-produced sexual imagery (also known as "sexting") refers to the creating, sharing, or possessing of nude or semi-nude images, videos, or live streams by children and young people under the age of 18.

This includes:

- Images or videos created by the young person themselves ("selfies")
- Images or videos created by others (including adults)
- Images or videos that have been digitally altered or created using artificial intelligence (e.g., deepfakes)
- Images or videos shared consensually (e.g., between partners)
- Images or videos shared non-consensually (e.g., as part of bullying, exploitation, or "revenge porn")

The Law

Creating, possessing, or sharing nude or semi-nude images of anyone under 18 is illegal, even if:

- The image is of yourself
- The image was shared consensually
- You are under 18 yourself

This is an offence under:

- **Protection of Children Act 1978** – creating or distributing indecent images of children
- **Criminal Justice Act 1988** – possessing indecent images of children
- **Sexual Offences Act 2003** – grooming and sexual exploitation

However:

- The police and schools recognise that young people may not understand the seriousness of their actions
- The police will use discretion and will not automatically criminalise young people
- The focus will be on safeguarding and education, not prosecution (unless there are aggravating factors, e.g., adult involvement, exploitation, malicious intent)

Why It's Harmful

Youth-produced sexual imagery can cause significant harm, including:

- **Emotional distress** – shame, embarrassment, anxiety, depression, suicidal thoughts
- **Bullying and harassment** – images can be shared widely and used to bully or blackmail
- **Exploitation** – images can be used by adults or peers to groom or exploit young people
- **Legal consequences** – young people can be investigated by the police and may be placed on the sex offenders register
- **Long-term impact** – images can resurface years later and affect future relationships, education, and employment

What Pupils Should Do

If you are asked to send a nude or semi-nude image:

- **Say no** – you have the right to refuse, even if the person is your boyfriend/girlfriend
- **Tell a trusted adult** – talk to a parent, teacher, or DSL
- **Block the person** if they continue to pressure you

If you receive a nude or semi-nude image:

- **Do not share it** – sharing it is illegal and can cause serious harm
- **Do not delete it** (yet) – it may be needed as evidence
- **Report it immediately** to a trusted adult (teacher, parent, DSL)

- **Do not screenshot or forward it** – this counts as sharing

If you have shared a nude or semi-nude image:

- **Tell a trusted adult immediately** – the sooner you tell someone, the sooner we can help
- **Do not panic** – you will not automatically get into trouble. We will support you and work with you to resolve the situation

How the School Will Respond

All incidents of youth-produced sexual imagery will be treated as safeguarding concerns and managed in line with our **Safeguarding and Child Protection Policy** and the **DfE guidance: Sharing nudes and semi-nudes (2020)**.

The school will:

1. Respond immediately

- The DSL will be informed immediately
- The incident will be recorded on CPOMS
- The pupil(s) involved will be supported and reassured

2. Assess the risk

The DSL will assess:

- The age of the pupils involved
- Whether the image was created, shared, or possessed voluntarily or under pressure
- Whether the image has been shared widely
- Whether there is an adult involved (e.g., grooming)
- Whether there are any aggravating factors (e.g., exploitation, malicious intent, significant age gap)

3. Decide whether to involve the police

The DSL will decide whether to involve the police based on the circumstances. The police **will** be involved if:

- There is an adult involved (e.g., grooming, exploitation)
- There is evidence of coercion, blackmail, or exploitation

- The images have been shared widely (e.g., on social media)
- The pupil is at risk of harm
- There are aggravating factors (e.g., significant age gap, malicious intent)

The police **may not** be involved if:

- The incident is low-risk (e.g., consensual sharing between peers of similar age, image not shared widely)
- The pupil is remorseful and understands the seriousness of their actions
- There are no aggravating factors

4. Support all pupils involved

Support for victims:

- Reassurance that they are not to blame
- Counselling or mentoring (via Pastoral Team or external agencies)
- Safety planning (e.g., blocking the perpetrator, monitoring social media)
- Regular check-ins to ensure they feel safe

Support for those who have shared images:

- Education about the seriousness of their actions and the harm caused
- Support to understand why they shared the image (e.g., peer pressure, relationship issues)
- Counselling or mentoring if there are underlying issues
- Monitoring to ensure the behaviour does not continue

5. Take appropriate action

Possible actions include:

- **Education** – helping pupils understand the seriousness of their actions
- **Restorative Justice** – where appropriate and agreed by all parties
- **Sanctions** – in line with the Behaviour Policy (e.g., detention, isolation)
- **Referral to external agencies** – e.g., CAMHS, social care, police
- **Removal of the image** – the school may confiscate devices and delete images (in line with Section 7)

6. Work with parents/carers

- Parents will be informed (unless this would put the pupil at risk)
- Parents will be involved in decisions about support and next steps
- Parents will be signposted to external support (e.g., CEOP, Internet Matters, NSPCC)

Viewing and Deleting Images

Staff must not:

- View youth-produced sexual imagery unless there is a clear safeguarding reason to do so (e.g., to assess the level of risk)
- Copy, print, or share the image

If a member of staff needs to view an image:

- This will be done by the DSL or Deputy DSL
- Another member of staff will be present as a witness
- The viewing will be recorded (including who viewed the image, when, and why)

Deleting images:

- If the image is held on a school device, the DSL may delete it (unless it is evidence of a criminal offence)
- If the image is held

DATA PROTECTION AND PERSONAL INFORMATION

Overview

South Shore Academy is committed to protecting the personal data of pupils, staff, parents, and visitors in line with the **Data Protection Act 2018** and **UK GDPR**.

This section provides a summary of our approach to data protection in relation to online safety. For full details, see our Data Protection Policy.

What is Personal Data?

Personal data is any information that can be used to identify a living individual, including:

- Names
- Addresses
- Email addresses
- Phone numbers
- Date of birth
- Photographs
- IP addresses
- Online identifiers (e.g., usernames, social media handles)

Special category data (which requires extra protection) includes:

- Ethnicity
- Religious beliefs
- Health information
- Biometric data (e.g., fingerprints)
- Sexual orientation

How We Protect Personal Data

We protect personal data by:

- **Storing data securely** – using encrypted systems, password-protected devices, and secure cloud storage
- **Limiting access** – only staff who need access to personal data for their role can access it
- **Training staff** – all staff receive data protection training as part of their induction and annually
- **Using secure communication systems** – school email, Google Workspace, and other official systems
- **Regularly reviewing data** – deleting data that is no longer needed
- **Reporting data breaches** – any data breaches are reported to the ICO (Information Commissioner's Office) within 72 hours if required

Protecting Pupil Data Online

Staff must:

- Not share pupil data via personal email, personal cloud storage, or personal devices
- Not share pupil data on social media (including in closed groups)
- Not discuss pupils in public places (including online forums or social media)
- Ensure pupil data is anonymised when used for educational purposes (e.g., case studies, training)

Pupils must:

- Not share personal information online (e.g., full name, address, phone number, school name)
- Not share other pupils' personal information online
- Use strong passwords and keep them private
- Report any concerns about data security to a trusted adult

Parents must:

- Not share other pupils' personal information on social media
- Not share images of other pupils without permission from their parents
- Respect the privacy of other families

Data Breaches

A data breach occurs when personal data is:

- Lost or stolen
- Accessed by unauthorised individuals
- Shared inappropriately (e.g., sent to the wrong person)
- Damaged or destroyed

If you become aware of a data breach, you must:

1. **Report it immediately** to the Data Protection Officer (DPO) or Headteacher
2. **Do not attempt to cover it up** or fix it yourself
3. **Preserve evidence** (e.g., take screenshots, save emails)

The school will:

- Investigate the breach
- Take steps to contain the breach and prevent further harm
- Notify affected individuals if necessary
- Report the breach to the ICO if required (within 72 hours)
- Review systems and procedures to prevent future breaches

Data Protection Officer (DPO): CIDARI MAT DPO

Subject Access Requests (SARs)

Individuals have the right to request access to their personal data held by the school (or their child's data, in the case of parents).

If you receive a subject access request, you must:

- Forward it to the DPO or Headteacher immediately
- Not attempt to respond yourself

The school will respond to SARs within one month.

For more information, see our Data Protection Policy.

EMERGING TECHNOLOGIES

Assessing New Technologies

Technology is constantly evolving, and new risks emerge regularly. South Shore Academy is committed to staying up to date with emerging technologies and assessing their risks before introducing them into school.

Before introducing a new technology (e.g., new app, platform, device, or system), we will:

1. **Assess the risks** – including safeguarding, data protection, and security risks
2. **Consult with stakeholders** – including the DSL, Online Safety Lead, IT Network Manager, and staff who will use the technology
3. **Review the terms and conditions** – ensuring the technology is appropriate for use in schools and complies with UK law
4. **Test the technology** – piloting it with a small group before rolling it out to all pupils/staff
5. **Provide training** – ensuring staff and pupils understand how to use the technology safely
6. **Monitor and review** – regularly reviewing the technology to ensure it remains safe and appropriate

Current Emerging Risks

The following are examples of emerging risks that we are monitoring:

Artificial Intelligence (AI)

- **Risks:** AI-generated content (e.g., deepfakes, AI-generated sexual imagery), misinformation, plagiarism, bias
- **Our approach:** Educating pupils about AI, teaching critical thinking skills, monitoring use of AI tools (e.g., ChatGPT)

Virtual Reality (VR) and Augmented Reality (AR)

- **Risks:** Exposure to inappropriate content, cyberbullying in virtual spaces, privacy concerns
- **Our approach:** Assessing VR/AR platforms before use, supervising pupils during use, educating pupils about risks

Live Streaming and Video Sharing Platforms

- **Risks:** Exposure to inappropriate content, grooming, cyberbullying, privacy concerns
- **Our approach:** Blocking access to live streaming platforms on the school network (unless required for educational purposes), educating pupils about risks

Gaming Platforms

- **Risks:** Grooming, cyberbullying, exposure to inappropriate content, excessive screen time, in-game purchases
- **Our approach:** Educating pupils and parents about gaming risks, blocking access to gaming platforms on the school network (unless required for educational purposes)

Cryptocurrency and NFTs

- **Risks:** Financial scams, gambling, exposure to illegal activity
- **Our approach:** Educating pupils about financial risks, monitoring online activity

"Sharenting" (Parents Sharing Images of Children Online)

- **Risks:** Privacy concerns, digital footprint, images being misused
- **Our approach:** Educating parents about the risks of oversharing, providing guidance on privacy settings

Reporting New Risks

If staff, pupils, or parents become aware of a new online risk or technology, they should report it to the Online Safety Lead or DSL immediately.

The Online Safety Lead will:

- Research the risk
- Assess the level of concern
- Communicate with staff, pupils, and parents if necessary
- Update the online safety curriculum and this policy if required

HOW THE SCHOOL WILL RESPOND TO ONLINE SAFETY ISSUES

Types of Incidents

Online safety incidents may include:

- Cyberbullying
- Youth-produced sexual imagery (sexting)
- Online grooming or exploitation
- Accessing inappropriate content (e.g., pornography, violence, self-harm, extremism)
- Sharing personal information online
- Hacking or unauthorised access to systems
- Breaches of the Acceptable Use Agreement
- Data breaches
- Inappropriate use of social media (by pupils, staff, or parents)

Response Procedures

All online safety incidents will be managed in line with our Safeguarding and Child Protection Policy and Behaviour Policy.

Step 1: Report

- All incidents must be reported immediately to the DSL or a member of staff
- Staff should not investigate incidents themselves (except to establish basic facts)

Step 2: Record

- The incident will be recorded on **CPOMS** with details of:
 - What happened (including dates, times, and who was involved)
 - What evidence was gathered (e.g., screenshots, witness statements)
 - What action was taken
 - Who was informed (e.g., parents, external agencies)

Step 3: Assess

The DSL will assess the incident to determine:

- **Is it a safeguarding concern?** (e.g., grooming, exploitation, self-harm)
- **Is it illegal?** (e.g., indecent images, threats, hate speech)

- **Who is at risk?** (the victim, other pupils, staff)
- **What is the level of risk?** (low, medium, high, immediate)
- **Do external agencies need to be involved?** (police, social care, CEOP, Prevent)

Step 4: Respond

The school will respond based on the assessment. Possible responses include:

For victims:

- Reassurance and emotional support
- Counselling or mentoring (via Pastoral Team or external agencies)
- Safety planning (e.g., blocking perpetrators, monitoring online activity, adjusting timetable)
- Regular check-ins to ensure they feel safe
- Referral to external agencies if needed (e.g., CAMHS, social care)

For those responsible:

- Education about the impact of their actions and how to make amends
- Restorative Justice (where appropriate and agreed by all parties)
- Sanctions in line with the Behaviour Policy (e.g., detention, isolation, exclusion)
- Counselling or mentoring if there are underlying issues
- Monitoring to ensure the behaviour does not continue
- Referral to external agencies if needed (e.g., police, social care, Youth Offending Team)

For parents:

- Parents will be informed (unless this would put the pupil at risk)
- Parents will be involved in decisions about support and next steps
- Parents will be signposted to external support

Step 5: Involve External Agencies (if necessary)

The school will involve external agencies where appropriate, including:

Agency	When to Involve	Contact
Police	Illegal activity (e.g., indecent images, threats, hate crimes, hacking)	101 (non-emergency) or 999 (emergency)
CEOP (Child Exploitation and Online Protection Centre)	Online grooming, exploitation, or indecent images	www.ceop.police.uk/safety-centre
Social Care	Child protection concerns (e.g., abuse, neglect, exploitation)	[Insert local contact, e.g., Blackpool Children's Services]
LADO (Local Authority Designated Officer)	Allegations against staff	[Insert local contact]
Prevent	Concerns about radicalisation or extremism	[Insert local Prevent contact]
CAMHS (Child and Adolescent Mental Health Services)	Mental health concerns (e.g., self-harm, suicidal thoughts)	[Insert local contact]
Anti-Terrorist Hotline	Immediate concerns about terrorism	0800 789 321

Step 6: Review

- The incident will be reviewed to identify any lessons learned and prevent future incidents
- The review will consider:
 - What happened and why
 - Whether the response was appropriate and effective
 - Whether any changes are needed to systems, procedures, or training
 - Whether any patterns or trends are emerging (e.g., repeated incidents involving the same pupils or types of behaviour)

Recording and Reporting

All online safety incidents are recorded on CPOMS and reviewed by the DSL.

The DSL will:

- Monitor trends and patterns
- Report serious incidents to the Headteacher and Governing Body
- Provide termly reports to the Senior Leadership Team and Governing Body on:
 - Number and types of incidents
 - Action taken
 - Lessons learned
 - Recommendations for improvement

TRAINING AND AWARENESS

Staff Training

All staff will receive online safety training:

- **During induction** for new staff
- **Annually** as part of safeguarding training (in line with KCSIE 2026)
- **Ad hoc** when new risks or technologies emerge

Training will cover:

- The school's online safety policy and procedures
- How to recognise online safety concerns (e.g., signs of cyberbullying, grooming, radicalisation)
- How to respond to online safety incidents
- How to teach online safety to pupils
- How to use technology safely and responsibly (e.g., email, social media, video conferencing)
- Staff responsibilities under the Acceptable Use Agreement and Staff Code of Conduct

Training will be delivered by:

- The DSL and Online Safety Lead
- External organisations (e.g., CEOP, local authority, NSPCC)

Staff must:

- Attend all online safety training
- Read and sign the Staff Acceptable Use Agreement annually
- Keep up to date with emerging risks and technologies

Governor Training

Governors will receive online safety training as part of their safeguarding training.

The Online Safety Governor will:

- Receive additional training on online safety
- Attend relevant conferences and events
- Keep up to date with emerging risks and technologies

- Report to the full Governing Body on online safety matters

Pupil Training

Pupils will receive online safety education as part of the curriculum (see Section 4).

Additional training will be provided:

- During induction for new pupils (e.g., Year 7 transition)
- During assemblies and Morning Meetings
- Through targeted interventions for vulnerable pupils

Parent Training

Parents will be offered online safety training through:

- Annual online safety workshops (e.g., during Safer Internet Day)
- Year 7 transition evening
- Information on the school website and in newsletters

Parents are encouraged to:

- Attend online safety workshops
- Talk to their children about online safety regularly
- Keep up to date with emerging risks and technologies

MONITORING AND REVIEW

Monitoring Arrangements

This policy will be monitored by:

- **The DSL and Online Safety Lead** – who will monitor online safety incidents, trends, and the effectiveness of the policy
- **The Senior Leadership Team** – who will review online safety provision and ensure the policy is being implemented consistently
- **The Governing Body** – who will receive annual reports on online safety and hold the Headteacher to account

Review Cycle

This policy will be reviewed **annually** by the **Senior Leadership Team** and **Governing Body** to ensure it remains effective and up to date with emerging risks and technologies.

The review will consider:

- Changes to legislation or guidance (e.g., updates to KCSIE)
- Emerging risks and technologies
- Feedback from staff, pupils, parents, and governors
- Online safety incidents and lessons learned
- Best practice from other schools and organisations

LINKS WITH OTHER POLICIES

This policy should be read in conjunction with:

- **Safeguarding and Child Protection Policy** – sets out our overall approach to keeping children safe
- **Behaviour Policy** – includes sanctions for misuse of technology and online behaviour
- **Anti-Bullying Policy** – includes our approach to cyberbullying
- **Data Protection Policy** – sets out how we handle personal data
- **Staff Code of Conduct** – includes expectations for staff use of technology and social media
- **Mobile Phone Policy (Pupils)** – sets out rules for pupils' use of mobile phones in school
- **Social Media Policy** – sets out how staff should use social media professionally

- **Acceptable Use Policies** (Appendices 1-3) – set out the rules for using technology in school
- **SEND Policy** – includes support for pupils with SEND in relation to online safety
- **PSHE Policy** – includes online safety education
- **Computing Curriculum** – includes technical aspects of online safety
- **Complaints Policy** – sets out how to raise concerns about the school

FURTHER INFORMATION AND SUPPORT

Internal Contacts

Designated Safeguarding Lead (DSL):

[Insert name]

 [Insert email]

 01253 336500

Deputy DSLs:

[Insert names and contact details]

Online Safety Lead:

[Insert name]

 [Insert email]

 01253 336500

IT Network Manager:

[Insert name]

 [Insert email]

 01253 336500

Headteacher:

Mr N Kay

 [Insert email]

 01253 336500

External Resources and Support

For Pupils:

- **Childline:** www.childline.org.uk | **Helpline: 0800 1111** (24/7, free, confidential)
- **CEOP (Report abuse):** www.ceop.police.uk/safety-centre
- **The Mix (under 25s):** www.themix.org.uk | **Helpline: 0808 808 4994**
- **Papyrus (suicide prevention):** www.papyrus-uk.org | **Helpline: 0800 068 4141**
- **Samaritans:** www.samaritans.org | **Helpline: 116 123** (24/7, free)

For Parents:

- **Internet Matters:** www.internetmatters.org – Age-specific advice and parental controls guides
- **NSPCC Online Safety:** www.nspcc.org.uk/keeping-children-safe/online-safety
- **UK Safer Internet Centre:** www.saferinternet.org.uk
- **Childnet:** www.childnet.com
- **Think U Know (CEOP):** www.thinkuknow.co.uk/parents
- **Net Aware (NSPCC & O2):** www.net-aware.org.uk – Social media guides for parents
- **National Cyber Security Centre:** www.ncsc.gov.uk/cyberaware

For Staff:

- **UK Safer Internet Centre:**
www.saferinternet.org.uk/advice-centre/teachers-and-school-staff
- **Childnet:** www.childnet.com/resources/teachers-and-professionals
- **CEOP Education:** www.thinkuknow.co.uk/professionals
- **Education Endowment Foundation:** educationendowmentfoundation.org.uk
- **UKCIS (UK Council for Internet Safety):**
www.gov.uk/government/organisations/uk-council-for-internet-safety

Reporting Concerns:

- **CEOP (Child Exploitation and Online Protection Centre):**
www.ceop.police.uk/safety-centre
- **Internet Watch Foundation (illegal content):** www.iwf.org.uk
- **Report Harmful Content:** reportharmfulcontent.com
- **Anti-Terrorist Hotline:** 0800 789 321

APPENDIX 1: ACCEPTABLE USE AGREEMENT – PUPILS

South Shore Academy – Pupil Acceptable Use Agreement

This agreement explains how you should use technology and the internet at South Shore Academy. Please read it carefully and sign at the bottom.

Using Technology Safely and Responsibly

I WILL:

- ☒ **Use school devices and the internet for learning** (unless I have permission to use them for other things, like at break time)
 - ☒ **Be kind and respectful online** – I will treat people the way I want to be treated
 - ☒ **Keep my personal information private** – I will not share my full name, address, phone number, or other personal details online
 - ☒ **Use strong passwords** and keep them secret (I can share them with my parents, but not with friends)
 - ☒ **Log out** of devices when I've finished using them
 - ☒ **Tell a trusted adult immediately** if I see or experience anything online that makes me feel uncomfortable, worried, or unsafe
 - ☒ **Ask for help** if I'm not sure whether something is safe or appropriate
 - ☒ **Follow the school's mobile phone rules**
-

I WILL NOT:

- ☒ **Access, create, or share inappropriate content** (like pornography, violence, or content that could upset or harm others)
- ☒ **Bully, harass, or be mean to others online** (cyberbullying)

- ✗ **Share or forward nude or semi-nude images** (even if they are of myself) – this is illegal and can cause serious harm
 - ✗ **Pretend to be someone else online** (impersonation)
 - ✗ **Share my password** with anyone (except my parents)
 - ✗ **Try to bypass the school's internet filters** (e.g., using proxy sites or VPNs)
 - ✗ **Download or install software, apps, or files** without permission from a teacher
 - ✗ **Use the internet for illegal activities** (like hacking, threats, or piracy)
 - ✗ **Share school login details** with anyone outside school
 - ✗ **Take photos or videos of other pupils or staff** without permission
-

What Happens If I Break the Rules?

If I break these rules, I understand that:

- I may face sanctions in line with the school's **Behaviour Policy** (e.g., detention, isolation, or exclusion)
 - My device may be confiscated and searched
 - My parents will be informed
 - The police may be involved if I have done something illegal
-

I Understand That:

- The school's online safety rules apply both in school and outside school (where they relate to the school community)
 - Some online activities are illegal and can have serious consequences
 - The school is here to help and support me, and I should always tell a trusted adult if I'm worried about something online
-

Agreement

I have read and understood this Acceptable Use Agreement. I agree to follow the rules and use technology safely and responsibly.

Pupil Name: _____ **Form:** _____

Pupil Signature: _____ **Date:** _____

Parent/Carer Signature: _____ **Date:** _____

APPENDIX 2: ACCEPTABLE USE AGREEMENT – STAFF

South Shore Academy – Staff Acceptable Use Agreement

This agreement sets out the expectations for staff use of technology and the internet at South Shore Academy. All staff must read and sign this agreement annually.

Professional Use of Technology

I WILL:

- ☒ Use school devices and the internet **professionally and responsibly**
- ☒ **Model safe and responsible use** of technology to pupils
- ☒ **Protect pupil data** and follow the school's **Data Protection Policy**
- ☒ Use **strong passwords** and keep them private
- ☒ **Log out** of devices when not in use
- ☒ **Report concerns immediately** to the DSL if I see or suspect online harm to a pupil
- ☒ Follow the school's **Social Media Policy** and **Staff Code of Conduct**
- ☒ Ensure all online communication with pupils is **professional** and takes place through **official school channels** (e.g., school email, Google Classroom)
- ☒ Seek permission before using **personal devices** for work purposes (and only in emergencies)

✓ Keep school devices **secure** when working remotely (e.g., at home)

✓ Report any **loss, theft, or damage** to school devices immediately

I WILL NOT:

✗ Access, create, store, or share **inappropriate content** (including pornography, violence, hate speech)

✗ Use school devices for **personal use** (except where explicitly permitted, e.g., checking personal email during breaks)

✗ **Share my password** with anyone (including colleagues or pupils)

✗ Attempt to **bypass the school's filtering or monitoring systems**

✗ Download or install **software, apps, or files** without permission from the IT Network Manager

✗ Use **personal devices** to communicate with pupils (e.g., personal mobile phone, personal email, personal social media)

✗ **Add pupils as "friends" or "followers"** on personal social media accounts

✗ **Share personal contact details** with pupils or parents (I will use school contact details only)

✗ **Take or share images of pupils** without following the school's procedures

✗ **Discuss pupils** on personal social media or in public places

✗ **Store pupil data** on personal devices or personal cloud storage (e.g., personal Google Drive, Dropbox)

Consequences of Breaching This Agreement

I understand that:

- Breaking these rules may result in **disciplinary action**, up to and including **dismissal**

- Serious breaches (e.g., accessing indecent images, grooming, data breaches) will be reported to the **police** and may result in referral to the **Disclosure and Barring Service (DBS)** and **Teaching Regulation Agency (TRA)**
-

I Understand That:

- Online safety is a **safeguarding issue**
 - I have a **duty to report concerns**, even if I am unsure
 - All use of school devices and the school network is **monitored**
 - I am responsible for **modelling safe and responsible use** of technology to pupils
-

Agreement

I have read and understood this Acceptable Use Agreement, the school's E-Safety & Online Safety Policy, and the Staff Code of Conduct. I agree to follow the rules and use technology professionally and responsibly.

Staff Name: _____ **Role:** _____

Staff Signature: _____ **Date:** _____

APPENDIX 3: ACCEPTABLE USE AGREEMENT – PARENTS/CARERS

South Shore Academy – Parent/Carer Acceptable Use Agreement

This agreement explains how parents and carers can support the school's online safety approaches. Please read it carefully and sign at the bottom.

Supporting Your Child's Online Safety

I WILL:

☒ **Support the school's online safety approaches** and reinforce online safety messages at home

- ✓ **Talk to my child regularly** about what they do online and who they talk to
 - ✓ **Set boundaries** around screen time and device use at home
 - ✓ **Use parental controls** on devices and internet connections
 - ✓ **Monitor my child's online activity** (e.g., check social media accounts, know their passwords)
 - ✓ **Be aware of the apps and games** my child is using
 - ✓ **Model safe and responsible use** of technology
 - ✓ **Report concerns** to the school if I am worried about my child's online activity or the online activity of other pupils
 - ✓ **Follow the school's social media policy** (e.g., not posting negative comments about the school, staff, or other pupils; not sharing images of other pupils without permission)
 - ✓ **Raise concerns directly with the school** (rather than posting on social media)
-

I WILL NOT:

- ✗ **Post negative, defamatory, or abusive comments** about the school, staff, or other pupils on social media
- ✗ **Share images of other pupils** on social media without permission from their parents
- ✗ **Share personal contact details** of staff or other families on social media
- ✗ **Take or share images** that could embarrass or upset pupils (e.g., in changing rooms, during sensitive moments)

I Understand That:

- The school takes online safety seriously and has systems in place to protect pupils
- My child's use of school devices and the school network is monitored for safeguarding purposes

- If my child misuses technology in a way that affects the school community, the school may take action (including sanctions and involving external agencies)
- The school is here to support families with online safety concerns

Agreement

I have read and understood this Acceptable Use Agreement. I agree to support the school's online safety approaches and follow the rules.

Parent/Carer Name: _____

Pupil Name: _____ **Form:** _____

Parent/Carer Signature: _____ **Date:** _____

APPENDIX 4: ONLINE SAFETY INCIDENT REPORT FORM

This form should be completed by staff when reporting an online safety incident. All incidents must be recorded on CPOMS and reported to the DSL immediately.

Incident Details

Date of incident: _____

Time of incident: _____

Reported by: _____ **Role:** _____

Date reported: _____

Pupil(s) Involved

Name(s) and form(s) of pupil(s) involved:

1. _____

2. _____
3. _____

Type of Incident (tick all that apply)

- ☐ Cyberbullying
- ☐ Youth-produced sexual imagery (sexting)
- ☐ Online grooming or exploitation
- ☐ Accessing inappropriate content (pornography, violence, self-harm, extremism)
- ☐ Sharing personal information online
- ☐ Hacking or unauthorised access
- ☐ Breach of Acceptable Use Agreement
- ☐ Data breach
- ☐ Inappropriate use of social media
- ☐ Other (please specify): _____

Description of Incident

Please provide a detailed description of what happened, including:

- What you saw or were told
- When and where it happened
- Who was involved
- Any evidence (e.g., screenshots, witness statements)

Evidence

Has evidence been saved? (e.g., screenshots, messages, images)

☐ Yes – evidence attached/saved on CPOMS

☐ No

If yes, please describe the evidence:

Immediate Action Taken

What action have you taken so far? (e.g., spoke to pupil, confiscated device, informed DSL)

Safeguarding Concerns

Do you have any safeguarding concerns about this incident?

☐ Yes

☐ No

If yes, please explain:

DSL Action (to be completed by DSL)

Date incident reviewed by DSL: _____

Risk assessment:

☐ Low risk

☐ Medium risk

☐ High risk

☐ Immediate risk

Action taken:

- ☐ Spoke to pupil(s) involved
- ☐ Informed parents
- ☐ Provided support to victim
- ☐ Sanctions applied (in line with Behaviour Policy)
- ☐ Referred to external agencies (please specify): _____
- ☐ Other (please specify): _____

Outcome:

DSL Signature: _____ **Date:** _____