Digital Safety Policy

2025 – 2026

Version Control	
Author	Glen Hookway (Regional Safeguarding Lead)
Version Number	01
Effective date	August 2025
Next review date	August 2026
Changes from previous version	Acceptable use policy (IT) and Digital Safety Policy are now separate documents (Safeguarding)

Previous Version	Author	Effective Date
01	Glen Hookway	
Approval		
Cognita Regional Office	OPSB	

Table of Contents

1. Introduction

1.1 We recognise that technology is an integral part of children's lives—used for learning, socialising, entertainment, and self-expression. While the digital world offers many opportunities, we also understand that children face significant risks online**.**

1.2 We should also recognise that risks linked to children being online are ever evolving, we must respond accordingly, adapting our approach to maintain the highest level of safeguarding and protection to our students.

1.3 We aim to educate, support and empower students to navigate the digital world safely, and to respond effectively to any concerns or incidents of online harm. The school actively promotes the participation of parents and guardians to help the school safeguard the welfare of students and promote the safe use of technology.

2. Purpose

2.1 To demonstrate the school's understanding of the risks and harms children may encounter online.

2.2 To ensure all staff are aware of their responsibilities in recognising, responding and reporting to any digital safety concerns by anticipating and preventing online risks arising from but not limited to:

- Exposure to harmful or inappropriate material (such as pornographic, racist, extremist, misogynistic or offensive material).
- Inappropriate contact from strangers and/or adults wishing to groom children for sexual or financial gain.
- Cyberbullying and abuse.
- Inappropriate taking and sharing of images and videos
- Cybercrime.

2.3 To outline the Monitoring and Filtering of school devices and network access for the purposes of Safeguarding, including the importance of effective collaboration between the IT Department and School Safeguarding Team.

2.4 To outline the importance of a responsive and dynamic Digital Safety curriculum, including the curriculum statement.

3. Scope

3.1 This policy applies to all students, staff, parents and visitors of the school.

3.2 This policy applies to concerns that occur on and off of school premises.

3.3 This policy applies to both school owned and privately owned devices.

3.4 This policy applies to incidents and concerns deriving from devices connected to the school network or personal 4G/5G.

4. Responsibilities

4.1 Staff are responsible for reading this policy and understanding the role they play within supporting children in keeping safe online.

4.2 The Head of School is responsible for ensuring that this policy is followed by all staff members.

4.3 The DSL/Safeguarding Team are responsible for managing all safeguarding concerns of students related to Digital Safety matters.

4.4 The Cognita Asia IT Director is responsible for ensuring that technology and IT Services contribute to keeping children safe online.

4.5 This policy will be reviewed and updated annually by the Regional Safeguarding Lead (RSL).

5. Monitoring and Filtering (for the purposes of Safeguarding)

5.1 Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

5.2 Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.

5.3 When a student is identified as attempting to access illegal, inappropriate or potentially harmful content online, a member of the IT team should inform the Designated Safeguarding Lead (DSL). This attempt may be part of a bigger picture of harm towards the child and/or a repeat of a previous abuse or harm towards the child. This information will allow the Safeguarding Team to put measures in place to protect the child or allow for Early Intervention if the child is unknown to the Safeguarding Team.

5.4 The IT team should produce a report of all sites that have been blocked and share with the Safeguarding Team regularly. This will allow trends and patterns to be tracked and if required additional measures implemented to address concerns raised, such as assemblies, changes to curriculum or pastoral support for those involved.

6. Safeguarding Children Online

6.1 It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

6.2 The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk.

7. Digital Safety Curriculum

7.1 As part of the schools PSHE/RSE Curriculum, students should be taught about online safety and harms. This includes being taught:

- What positive, healthy and respectful online relationships look like
- The effects of their online actions on others
- How to recognise and display respectful behaviour online
- How to use technology safely, responsibly, respectfully and securely
- Where to go for help and support when they have concerns about content or contact on the internet or other online technologies

7.2 Throughout these topics, teachers will assess online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives.

7.3 The school's Digital Safety Curriculum should be reactive to the needs of the students. The voice of the student is integral in understanding the potential risks they are facing, meaning the curriculum should be responsive and dynamic.

7.4 Primary and Secondary PSHE follows the Jigsaw curriculum. In addition to this, this academic year the Digital Learning and PSHE team are working towards becoming a Common Sense Media School.

8. Use of Mobile Phones/Devices

8.1 Every school has a duty to create an environment that is calm, safe and free from distraction so all pupils can learn and thrive. One of the greatest challenges facing schools is the presence of mobile phones, which can be used for the purposes of carrying out abus or harm. Therefore, schools must have clear guidelines on the use of mobile phones which aligns with your school Behaviour Policy, Anti-Bullying Policy and International Safeguarding Policy.

8.2 Primary students are not permitted to bring smart watches or mobile phones to school. In Year 5 and 6 students are able to bring their own devices with permission.

8.3 Secondary students may bring their own devices and mobile phones to school. They are able to use them within lessons with the teachers permission, otherwise they must be stored securely in their locker. Devices must not be used in social/ communal areas.

9. Photographs, Images and videos

9.1 The school abides by all relevant personal data protection legislation and the school's own Personal Data Protection Policy.

9.2 Schools understand that an image or video is considered personal data. It will seek written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes, such as a yearbook or on a parent portal. Parents and guardians may withdraw this permission at any time by informing the school in writing. When seeking parental consent, the school should also make clear how parents can write in to withdraw consent.

9.3 Staff, students, parents and visitors are not permitted to use devices such as mobile phones, cameras, smart watches or digital recorders to photograph or record members of staff or students without permission. Permission may be granted by the school in the event of performances/events organised by the school.

9.4 When permission is granted by the school, parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of children other than their own in any public forum without the permission of the relevant family. It is illegal to sell or distribute recordings from events without permission. Any parent who does not wish for their child to be videoed or photographed at school events by other attendees must notify the school in advance and in writing.

9.5 Schools to have clear and published procedures for the retention and deletion of photos, images, and videos. There must be a valid reason, for example, history of school, for keeping images over an extended period.

9.6 The annual safeguarding declaration will include a statement saying that any photos or videos residing on personal devices have been deleted from the device and personal cloud storage.

9.7 Staff should receive a reminder from the school toward the end of each semester to delete all images from personal devices and cloud storage.

9.8 Staff must abide by professional standards and comply with this policy.

10. Use of Personal Equipment to take photos/images/videos in School

10.1 The use of school devices to capture images of students will be the normal practice. Personal devices are not to be used for this purpose.

10.2 Occasionally a personal device may be used for a specific and agreed purpose in line with school policy. This may vary from school to school and will require explicit approval at school level.

10.3 For example, an image, for use in the classroom as a learning enhancement, can be used if the school has permission from all parents of the students in the image.

10.4 Schools may choose to only allow staff to use photos taken in school that contain no images of children or to not allow staff to use any images on their professional social media accounts.

10.5 Schools may allow staff to take an image of a student or an event which is for sole use by the communication team, after clearing with the compliance officer, on a school social media account.

11. Knowledge Base

Cyber-Bullying

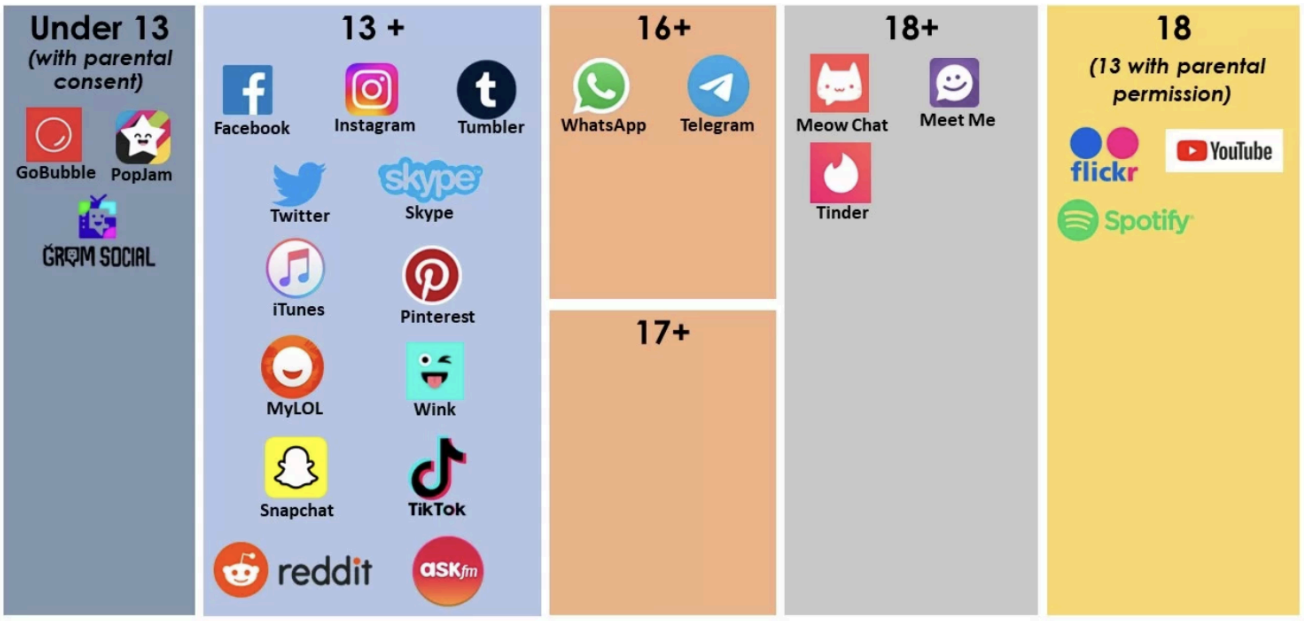
Bullying is behaviour that is deliberate, repeated more than once and is designed to be hurtful. This type of behaviour can happen both on and offline (and often both), so it is crucial to consider all associated behaviour. Refer to the schools Anti-Bullying Policy to effectively manage concerns of Cyber-Bullying. Unlike face-to-face bullying, cyberbullying can happen at any time, often anonymously, and can quickly spread to a wide audience, making it particularly distressing for the victim. Children who experience cyberbullying may feel isolated, anxious, or depressed, and in some cases, it can lead to self-harm or withdrawal from school life.

Sexting/ Inappropriate Images & Videos (Including AI)

Sexting is a term which describes the sharing of intimate images with others, using online technologies. Sexting is an increasing phenomenon among children, even of primary age and remains a significant area of concern. To support schools in effectively managing concerns of sexting and/or the sharing/receiving of inappropriate images and videos please read the Recognising & Responding to Sharing Nudes & Deepfakes Guide for Schools. Even if shared voluntarily, once an image is sent, control over it is lost, and it can be copied, shared, or posted online without consent. This can lead to embarrassment, bullying, blackmail, or long-term damage to a young person's reputation and mental health. In some cases, sexting may also involve coercion or pressure from peers or adults, and the creation or possession of explicit images of anyone under 18 can be a criminal offence.

Social Media

Social media presents a range of risks for children and young people, including exposure to inappropriate content, cyberbullying, online grooming, and the sharing of personal information. The nature of social platforms can make it difficult to verify identities, increasing the risk of contact with strangers who may have harmful intentions. In addition, the pressure to gain likes and followers can negatively impact students' mental health and self-esteem. Schools should be aware of the age requirements in accessing various social media platforms in the country they are working in.



Inappropriate Material (Including 18+ rated games and films)

Exposure to inappropriate material, including 18+ rated games and films, poses significant risks to children and young people. Such content may contain violence, explicit language, sexual content, or harmful stereotypes that are not suitable for

their age or level of maturity. Regular exposure can desensitise children to aggressive or unsafe behaviours, distort their understanding of healthy relationships, and negatively influence their emotional and psychological development. It may also increase anxiety, fear, or confusion, particularly if children do not have the tools or support to process what they have seen. Incidents of children viewing inappropriate material is a safeguarding concern and the International Safeguarding Policy should be referred to if you have any concerns.

Online Grooming & Exploitation

Online grooming and exploitation are serious risks that can occur when children and young people are targeted by individuals with harmful intentions through digital platforms. Offenders may use social media, gaming chats, or messaging apps to build trust with a child, often by pretending to be someone they are not. Over time, they may manipulate the child into sharing personal information, images, or meeting in person, putting them at risk of emotional, physical, or sexual harm. Grooming can be difficult to recognise, as it often involves secrecy and manipulation. Incidents of Grooming and Exploitation are safeguarding concerns and the International Safeguarding Policy should be referred to if you have any concerns.

Online Radicalisation & Extremism

Radicalisation is the process by which individuals come to adopt extreme political, social, or religious ideologies—often through exposure to content, communities, or individuals on the internet. This can lead them to support or engage in violence, terrorism, or other forms of extremist behaviour. It often happens through social media, forums, messaging apps, or video platforms, where people may be targeted or influenced by extremist propaganda, misinformation, or peer pressure. Refer to the schools Preventing Radicalisation & Extremism Policy to effectively manage concerns of Radicalisation and Extremism.

Cybercrime

Children and young people are increasingly becoming targets of online scams due to their growing digital presence and lack of experience in recognising fraudulent activity. These scams can lead to emotional distress, financial loss, or the unintentional sharing of personal or sensitive information. Incidents involving Cybercrime is a safeguarding concern and the International Safeguarding Policy should be referred to if you have any concerns.

12. Procedures for Reporting

12.1 All concerns regarding potential harm of a child in relation to being online must be reported as soon as possible using CPOMS.

12.2 If appropriate you may take screenshots or photos of text that may support the identification of a perpetrator or supports to protect a victim. However, you must never take screenshots or photos of images that are inappropriate in nature. If known, inform the DSL when reporting that images exist and where they may be located (i.e. on a student's phone).

12.3 If you have a concern regarding inappropriate use of Digital Devices of an adult associated with the school that indicates they may pose a risk of harm to a child, complete a Low-Level Concern Form as soon as possible. If the concern involves grooming, sexual harm of a child or radicalisation then speak directly with the Head of School immediately.

13. Self-Assessment

13.1 A vital component of effective Safeguarding is to regularly review and assess our systems designed to keep children safe from harm online, as well as learning lessons when a child or children have suffered harm, neglect or exploitation. It is therefore essential that our online systems are assessed for the purposes of continued improvement. Lessons Learned reviews should be carried out in any cases where a child or children have been harmed online and/or from using digital devices at our school.

14. Acceptable Use Agreements

14.1 Acceptable Use Agreements are essential tools within the school's Digital Safety Framework and must be read in conjunction with the Digital Safety Policy. See the Acceptable Use Agreement Policy for more detail.

14.2 The Acceptable Use Agreement outlines:

- What is allowed and not allowed when using school ICT systems, WI-FI, online platforms apps and devices.
- Consequences of misuse or breaches of digital safety expectations.