Inspire Partnership Academy Trust

West Thornton
PRIMARY SCHOOL

# Online Safety Policy

September 26/27

| | |
|---|---|
| Approval Date: | October 2026 |
| Approved by: | Trust Board |
| Policy Owner: | Stephen Schwartz |
| Review date: | September 2026 |

## Table of Contents

Table of Contents 2

Table of Contents 2
1. Introduction 4
1.1. Key people and dates 4
1.2. What is this policy? 6
1.3. Who is it for; when is it reviewed? 6
1.4. Who leads online safety? 7
1.5. What were the main online safety risks in 2025/2026? 7
1.5.1. There are 4 types of online safety risks outlined in KCSIE: 7
1.6. Online Safeguarding Trends at West Thornton Primary School 8
1.7. How will this policy be communicated? 8
2. Overview 8
2.1. Aims 8
2.2. Further Help and Support 10
3. Scope 10
4. Roles and responsibilities 10
5. Education and curriculum 11
6. Handling safeguarding concerns and incidents 12
6.2. Actions where there are concerns about a child 14
6.3. Sharing nudes and semi-nudes 15
6.3.4. Consider the 5 points for immediate referral at initial review: 16
6.4. Upskirting 17
7. Bullying 17
8. Child-on-child sexual violence and sexual harassment 18
9. Misuse of school technology (devices, systems, networks or platforms) 18
10. Social media incidents 19
11. Data protection and cyber security 19
12. Appropriate filtering and monitoring 20
13. Use of generative AI 21

14. Messaging/commenting systems (incl. email, learning platforms & more) 23
14.1. Authorised systems 23
14.2. Behaviour / usage principles 24
14.7. Online storage or learning platforms 24
15. School website 25
15.3. Digital images and video 25
16. Social media 27
16.1. Our SM presence 27
16.2. Staff, pupils' and parents' SM presence 28
17. Device usage 30
17.2. Personal devices including wearable technology and bring your own device (BYOD) 31
17.3. Use of school devices 32
18. Trips / events away from school 32
19. Searching and confiscation 33
20. Extremism 33
21. CCTV 33
1. Appendix A 35
1.1. Roles 35
1.1.2. All staff 35
1.1.6. Head Teacher 36
1.1.7. Designated Safeguarding Lead / Online Safety Lead – Donna Callaghan 37
1.1.7.1. Key responsibilities (remember the DSL can delegate certain online-safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education): 37
1.1.8. Trustees, Trust Education Leads and Local Community Councils (LCC) 39
1.1.8.8. Key responsibilities: 40
1.1.9. PSHE / RHE Lead/s - {{PSHE_LEAD_NAME}} 42
1.1.9.1. Key responsibilities: 42
1.1.10. Computing Lead - {{COMPUTING_LEAD_NAME}} 43
1.1.10.1. Key responsibilities: As listed in the 'all staff' section, plus: 43
1.1.11. Subject leaders 43
1.1.11.1. Key responsibilities as listed in the 'all staff' section, plus: 43
1.1.12. Network Manager/other technical support roles - Turn IT On 44

1.1.12.1. Key responsibilities as listed in the 'all staff' section, plus: 44
1.1.13. Data Protection Officer (DPO) - Stephen Schwartz / DPO centre 45
1.1.13.1. Key responsibilities: 45
1.1.14. Volunteers and contractors (including tutors) 46
1.1.14.1. Key responsibilities: 46
1.1.15. Pupils 47
1.1.15.1. Key responsibilities: 47
1.1.16. Parents/carers 47
1.1.16.1. Key responsibilities: 47
1.1.17. External groups including parent associations 47
2. Appendix B: The National Landscape of Online Safety 48
2.2. National Online Safeguarding Trends
. 48
2.2.2. LGfL Senso monitoring data has also revealed other concerns in schools: 49

# 1. Introduction

## 1.1. Key people and dates

| Role | Details |
|---|---|
| School Name | West Thornton Primary School |
| Designated Safeguarding Lead (DSL) | Donna Callaghan |
| Deputy Designated Safeguarding Leads / DSL | Clare Dennis<br>Lisa Gallagher |

| Role | Details |
|---|---|
| Team Members | Leah Hefetz<br>Shama Abraham<br>Laura Little<br>Jennifer McKenna<br>Rachel Greene<br>Alicia Williams<br>Recaina Liburd |
| Link LLC member for safeguarding | Tim Barnes |
| Network manager / other technical support | Turn IT On |
| Date this policy was reviewed and by whom | October 2026 |
| Date of next review and by whom | September 2027 / Stephen Schwartz |

## 1.2. What is this policy?

1.2.1. Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2026 (KCSIE), 'Teaching Online Safety in Schools', statutory RHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

## 1.3. Who is it for; when is it reviewed?

1.3.1. This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, LCC members, pupils and parents in writing and reviewing the policy and making sure the policy makes sense and it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

## 1.4. Who leads online safety?

1.4.1. KCSIE makes clear that "the Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)." The DSL can delegate activities but not responsibility for this area, and whilst

subject leads (e.g. for RSHE) will plan the curriculum for their area, it is important that this ties into a whole-school approach.

## 1.5. What were the main online safety risks in 2025/2026?

### 1.5.1. There are 4 types of online safety risks outlined in KCSIE:

1.5.1.1. CONTENT: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

1.5.1.2. CONTACT: being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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,

1.5.1.3. CONDUCT: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and

1.5.1.4. COMMERCE: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

1.5.2. It is the responsibility of all staff to understand the above, recognise when a child may be experiencing harm related to the above, and report to the DSL.

## 1.6. Online Safeguarding Trends at West Thornton Primary School

1.6.1. In our school over the past year, we have noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our pupils:

Inappropriate use of WhatsApp

Accessing inappropriate content

### 1.7. How will this policy be communicated?

1.7.1. This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

1.7.1.1. Posted on the school website

1.7.1.2. Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)

1.7.1.3. Integral to safeguarding updates and training for all staff

1.7.1.4. Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, LCC members, pupils and parents/carers), which will be issued to the whole school community, on entry to the school, annually and whenever changed and shared on the school website. Discussed in parent webinars/workshops.

## 2. Overview

### 2.1. Aims

2.1.1. This policy aims to promote a whole school approach to online safety by:

2.1.1.1. Setting out expectations for all West Thornton Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

2.1.1.2. Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RHE) and beyond.

2.1.1.3. Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.

2.1.1.4. Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.

2.1.1.5. Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world;

2.1.1.5.1. for the protection and benefit of the children and young people in their care, and for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice,

2.1.1.5.2. for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession,

2.1.1.5.3. Establishing clear structures by which online misdemeanors will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

## 2.2. Further Help and Support

2.2.1. Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also

have advisors to offer general support.

2.2.2. Beyond this, reporting.lgfl.net has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

## 3. Scope

3.1.1. This policy applies to all members of the West Thornton Primary School community (including teaching, supply and support staff, LCC members, volunteers, contractors, pupils/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

## 4. Roles and responsibilities

4.1.1. This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behavior, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

4.1.2. Depending on their role, all members of the school community should read the relevant section in Appendix A of this document that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the appendix. All staff have a key role

to play in feeding back on potential issues.

## 5. Education and curriculum

5.1.1. It is important that schools establish a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

5.1.2. As well as teaching about the underpinning knowledge and behaviors that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, Teaching Online Safety in Schools recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

5.1.3. Online safety will be taught through the Computing and RHE elements of the Inspire Partnership Curriculum - https://sites.google.com/inspirepartnership.co.uk/croydoncurriculum/home?authuser=0

5.1.4. Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and conspiracy theories in line with KCSIE 2025), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

5.1.5. At West Thornton Primary School, we recognize that online safety and broader digital resilience must be a thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework ‘Education for a Connected World – 2020 edition’ from UKCIS (the UK Council for Internet Safety) through the use of the Project Evolve materials created by the UK Safer Internet Centre.

5.1.6. Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership. https://sites.google.com/inspirepartnership.co.uk/croydoncurriculum/subject-progression-documents

5.1.7. This is done within the context of an annual online safety audit, which is a collaborative effort led by Stephen Schwartz (Trust EdTech Lead), Donna Callaghan (HT/DSL), Clare Dennis (DDSL) and Mohamed Kamara (Computing Lead)

## 6. Handling safeguarding concerns and incidents

6.1.1. It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RHE and Citizenship). General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

6.1.2. Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

6.1.3. School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

6.1.3.1. Safeguarding and Child Protection Policy (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=793&type=pdf)

6.1.3.2. Anti-Bullying Policy (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=797&type=pdf)

6.1.3.3. Behaviour Policy (including school sanctions) (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=791&type=pdf)

6.1.3.4. Acceptable Use Policies (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=806&type=pdf)

6.1.3.5. Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc) (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=584&type=pdf)

6.1.4. This school commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

6.1.5. Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

6.1.6. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of the Local Community Council and the LADO (Local Authority's Designated Officer).

6.1.7. The school and Trust will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice

and related legal duties including support for pupils and powers of staff when responding to incidents

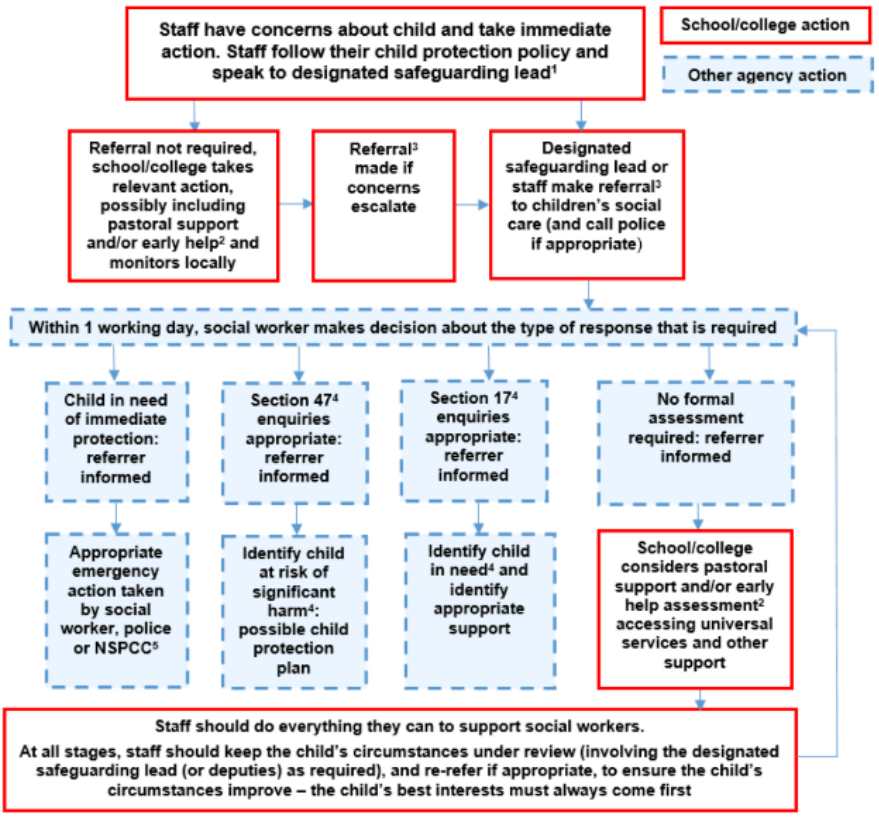
6.1.8. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sharing nudes (or semi nudes) and upskirting; see section below).

6.1.9. The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

## 6.2. Actions where there are concerns about a child

6.2.1. The following flow chart is taken from page 26 of Keeping Children Safe in Education 2026 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern. Crucially, as per the Children's Wellbeing and Schools Act (2026), there is now a mandatory duty for teachers to report any concerns of child sexual abuse, which includes sexual abuse that is facilitated by and/or takes place online (including non-contact abuse such as image sharing). Therefore, all staff must report such concerns without delay to the DSL.

**Figure 1 Flowchart : actions taken where there are concerns about a child**




## 6.3. Sharing nudes and semi-nudes

6.3.1. All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

6.3.2. There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an

incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

6.3.3. The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.

### 6.3.4. Consider the 5 points for immediate referral at initial review:

6.3.4.1. The incident involves an adult

6.3.4.2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)

6.3.4.3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent

6.3.4.4. The images involves sexual acts and any pupil in the images or videos is under 13

6.3.4.5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

6.3.5. It is important that everyone understands that whilst sharing nudes and semi-nudes is illegal, pupils/pupils can come and talk to members of staff if they have made a mistake or had a problem in this area. The documents referenced above and materials to support teaching about sharing nudes and semi-nudes (sexting) can be found at sexting.lgfl.net

### 6.4. Upskirting

6.4.1. It is important that everyone understands that upskirting (taking a photo or video of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

6.4.2. Staff and pupils must be aware that upskirting has become more prevalent due to the increased use of smart glasses and other discreet recording technology that can capture imagery without individuals knowing.

## 7. Bullying

7.1.1. Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

7.1.1.1. Anti-Bullying Policy: https://www.inspirewestthornton.co.uk/attachments/download.asp?file=797&type=pdf

7.1.2. It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

7.1.3. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net.

## 8. Child-on-child sexual violence and sexual harassment

8.1.1. Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviors incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviors such as bra-strap flicking and the careless use of language.

## 9. Misuse of school technology (devices, systems, networks or platforms)

9.1.1. Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Acceptable Use Policy (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=806&type=pdf) as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

9.1.2. Where pupils contravene these rules, the school behavior policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook. (https://www.inspirewestthornton.co.uk/information/policies)

9.1.3. It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place.

9.1.4. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

## 10. Social media incidents

10.1.1. Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies/social media policy/online safety.

10.1.2. Breaches will be dealt with in line with the school behavior policy (for pupils) or code of conduct/handbook (for staff).

10.1.3. See the social media section later in this document for rules and expectations of behavior for children and adults in the West Thornton Primary School community.

10.1.4. Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), West Thornton Primary School will request that the post be deleted and will expect that to be actioned promptly.

10.1.5. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

## 11. Data protection and cyber security

11.1.1. All pupils, staff, LCC members, volunteers, contractors and parents are bound by the school's data protection policy which can be found here;

11.1.1.1. https://www.inspirewestthornton.co.uk/attachments/download.asp?file=584&type=pdf

11.1.2. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cyber Security for Schools and Colleges.

11.1.3. Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for

consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2025, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

## 12. Appropriate filtering and monitoring

12.1.1. The designated safeguarding lead (DSL) Donna Callaghan has lead responsibility for filtering and monitoring and works closely with Turn IT On to implement the DfE filtering and monitoring standards, which require schools to

12.1.2. identify and assign roles and responsibilities to manage filtering and monitoring systems

12.1.3. review filtering and monitoring provision at least annually and carry out half-termly checks to ensure filtering is operational, functioning as expected, and that the school responds to issues

12.1.4. block harmful and inappropriate content without unreasonably impacting teaching and learning

12.1.5. have effective monitoring strategies in place that meet their safeguarding needs, including SENSO real-time monitoring triggered by inappropriate keystrokes or attempts to access blocked sites

12.1.6. We look to provide appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times. The school uses LGfL filtering, please visit appropriate.lgfl.net for more information.

12.1.7. We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential overblocking. They can submit concerns at any point via https://docs.google.com/forms/d/e/1FAIpQLSfNCQ6jaFufkVFP8wgtwk8T4qSmcpM1HgaQPOjv5Nf7n5yyMA/viewform and will be asked for feedback at the time of the regular checks which will now take place.

12.1.8. Technical and safeguarding colleagues work together closely to carry out annual reviews and checks and also to ensure that the school responds to

issues and integrates with the curriculum.

12.1.9. We carry out half-termly checks to ensure filtering is operational, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc. More details of both documents and results are available on request dependent on staff roles from

12.1.10. We know that what children input and what the tool outputs cannot be guaranteed as safe, so we carefully monitor output via SENSO and limit their use in line with DfE guidelines. Please note that even with Safe Search enforced, AI is embedded in many search engine responses and this presents risks to users in terms of misinformation, bias, hallucinations, and inappropriate content.

12.1.11. Safe Search is enforced on any accessible search engines on all school-managed devices

12.1.12. Our YouTube mode is safe search for pupils (check with TIO). This helps us to limit inappropriate content that is served to pupils

12.1.13. Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

12.1.14. The DSL checks filtering reports and notifications Weekly and takes any necessary action as a result.

12.1.15. The school has implemented SENSO which provides real time monitoring which is triggered by inappropriate keystrokes or attempts to access blocked sites. The site records who, the words/site and a screen shot so that false positives can be identified and action taken where positive results are seen. This is checked by the DSL Weekly.

## 13. Use of generative AI

13.1.1. The Trust provides Google Gemini as its standard generative AI platform for staff use through Trust-managed accounts. The Trust also recognises that different generative AI platforms may offer different functionality and professional benefits. Where there is a clear rationale for using an alternative

platform, this may be considered through the Trust's agreed approval process.

13.1.2. Requests should normally be made by a Headteacher or central Trust leader on behalf of themselves or their team and will be subject to appropriate technical, safeguarding and data-protection assurance, including a DPIA where required.

13.1.3. We foster a culture of safe innovation where staff are encouraged to explore how emerging technologies can enhance teaching, learning and organisational effectiveness. Leaders will provide clear guidance, appropriate professional development and proportionate assurance processes so that innovation can take place without compromising pupil or staff privacy, security, safeguarding or regulatory compliance.

13.1.4. When using Google Gemini, staff must access the platform using their Trust Google account. Where staff use another Trust approved generative AI platform, it must be accessed and used in accordance with any account, security and data-protection requirements specified as part of the Trust's approval process. Staff must not enter personal, sensitive or confidential information relating to pupils, staff or the Trust unless its use for that purpose has been explicitly approved through the Trust's data-protection processes.

13.1.5. The school has a clear and well communicated approach to the use of any Gen AI (by staff or pupils), and this is aligned with the school's values and pedagogical approaches.

13.1.6. To help users to safely use technology, we will talk about the use of these tools with pupils, staff and parents – their practical use as well as their safety and ethical pros and cons.

13.1.7. We are aware that there will be use of these apps and exposure to Gen AI creations on devices at home for many pupils – these experiences may be both positive/creative and also negative (e.g. data breaches, misinformation, bullying, deep fakes, creation of deepfake intimate imagery and chatbots that encourage unhealthy and inappropriate relationships). Therefore, it is important as a school that we support pupils in developing digital literacy skills to help mitigate these risks.

# 14. Messaging/commenting systems (incl. email, learning platforms & more)

## 14.1. Authorised systems

14.1.1. Pupils at this school communicate with each other and with staff using Google Classroom only.

14.1.2. Staff at this school use the email system provided by Google for Education and / or Arbor for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with parents, external organisations and professional activity.

14.1.3. Email should never be used to communicate with pupils.

14.1.4. Staff at this school primarily use Arbor MIS to communicate with parents through email and the Arbor Parent App.

14.1.5. Any systems above are centrally managed and administered by the Trust. This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

14.1.6. Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and central leadership team.

14.1.7. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

14.1.8. Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

14.1.9. Any data loss should be recorded here - https://docs.google.com/forms/d/e/1FAIpQLSfyF3dRQhzL2ti34EXn-SrQPlirqEfEakn7xI7R5qHhoLvYXw/viewform

### 14.2. Behaviour / usage principles

14.3. More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements, behavior policy and staff code of conduct.

14.4. Appropriate behavior is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

14.5. Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=584&type=pdf) and only using the authorised systems mentioned above.

14.6. Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behavior apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

## 14.7. Online storage or learning platforms

14.8. All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc. In [Insert School Name] this includes;

14.8.1. CPOMs - safeguarding
14.8.2. Arbor
14.8.3. Google for Education
14.8.4. Canva

14.8.5. SamPeople HR

14.9. For all these, it is important to consider data protection and cyber security before adopting such a platform or service and at all times when using it. Any new platforms will be approved by the headteacher and the central leadership team

## 15. School website

15.1. The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher/Principal and LCC members have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to our office teams (alongside Donna Callaghan & Clare Dennis - Headteacher).

15.2. Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with the Innovation and EdTech lead in the central team.

### 15.3. Digital images and video

15.3.1. When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. In light of image manipulation by Gen AI platforms to create sexual imagery of children and adults, the school follows the UK Online Harms Early Warning Working Group guidance (May 2026).

15.3.2. To mitigate the risk of data breaches and safeguarding incidents, we will avoid publishing and sharing any high-resolution images of children's faces on our

website, social media, or marketing materials, and will instead publish lower-resolution images of children from behind or in group shots.

15.3.3. The school leadership team will ensure that staff in the school are made aware of the risk associated with the AI manipulation of images and will employ the mitigations listed.

15.3.4. Parents answer as follows: (edit as necessary)

15.3.4.1. For displays around the school
15.3.4.2. For the newsletter
15.3.4.3. For use in paper-based school/Trust marketing
15.3.4.4. For online prospectus or websites
15.3.4.5. For social media and press coverage of the school or school Trust
15.3.4.6. For a specific high-profile image for display or publication

15.3.5. Whenever a photo or video is taken/made, the member of staff taking it will check the latest database on Arbor before using it for any purpose. Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

15.3.6. All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At West Thornton Primary School, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

15.3.7. Staff and parents are reminded annually about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

15.3.8. We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

15.3.9. Pupils are taught about how images can be manipulated in their online safety education program and also taught to consider how to publish for a wide range of audiences which might include LCC members, parents or younger children.

15.3.10. Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

15.3.11. Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

15.3.12. Parents must not covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous (see nofilming.lgfl.net for more information).

# 16. Social media

## 16.1. Our SM presence

16.1.1. West Thornton Primary School works on the principle that if we don't manage our social media reputation, someone else will.

16.1.2. Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

16.1.3. Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

16.1.4. Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner. The leadership team is responsible for managing our X-Twitter/Facebook/Instagram and other social media accounts and checking our Wikipedia and Google reviews and other mentions online.

## 16.2. Staff, pupils' and parents' SM presence

16.2.1. Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

16.2.2. This positive behavior can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

16.2.3. If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure (https://www.inspirewestthornton.co.uk/attachments/download.asp?file=768&type=pdf) should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

16.2.4. Many social media platforms have a minimum age of 13 but the school regularly deals with issues arising on social media involving pupils/pupils under

the age of 13. **However, as of June 2026, the UK Government has announced that social media will be banned for under 16-year-olds. The school is beginning preparations for this transition, including how to manage reports of children accessing social media and how to support parents.** While navigating this change, we ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

16.2.5. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/pupils to avoid or cope with issues if they arise.

16.2.6. Online safety lessons will look at social media and other online behavior, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behavior they see and experience, which will often be from adults.

16.2.7. Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

16.2.8. Although the school has an official X-Twitter and Instagram account and will respond to general inquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

16.2.9. Email / Arbor Parent App is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

16.2.10. As outlined in the Acceptable Use Policies, pupils/pupils are not allowed to be 'friends' with or make a friend request to any staff, LCC members, volunteers and contractors or otherwise communicate via social media.

16.2.11. Pupils/pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we accept that this can

be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

16.2.12. Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal and should be declared upon entry of the pupil or staff member to the school).

16.2.13. Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

16.2.14. Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

16.2.15. The serious consequences of inappropriate behavior on social media are underlined by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

16.2.16. All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people.

## 17. Device usage

17.1.1. AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUPs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

## 17.2. Personal devices including wearable technology and bring your own device (BYOD)

17.2.1. Pupils/pupils in Year 5 & Year 6 are allowed to bring mobile phones in for emergencies and travelling between school and home.

17.2.2. Personal recording devices, such as smart glasses, are not permitted in school without written permission. It is strictly forbidden to take secret photos, videos, or recordings of teachers or pupils, including remotely, with any device. This applies to staff, pupils, parents, volunteers, and contractors.

17.2.3. Apple AirTags or similar tracking devices are allowed for personal use by adults (on car keys etc). However please note that it is against the terms and conditions of these products to use them to track a child, and they could present a risk to the safety of all pupils.

17.2.4. All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies.

17.2.5. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

17.2.6. Volunteers, contractors, LCC members should leave their phones in their pockets and turn them off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

17.2.7. Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page.

17.2.8. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

17.2.9. Neither staff nor pupils are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs. The only exception being where there is a temporary internet outage and the headteacher has approved this use.

### 17.3. Use of school devices

17.3.1. Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behavior when on school devices, whether on site or at home.

17.3.2. Staff should not use a personal laptop or computer for work in school, The school provides devices.

17.3.3. School devices are not to be used in any way which contravenes AUPs, behavior policy / staff code of conduct.

17.3.4. Wi-Fi is accessible to staff for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

17.3.5. School devices for staff or pupils are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

17.3.6. All and any usage of devices and/or systems and platforms may be tracked.

## 18. Trips / events away from school

18.1.1. For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

18.1.2. If on trips pupils are encouraged to connect to another organisation's Wi-Fi/network, staff must be aware that other connections may not be as well controlled (e.g. via filtering and monitoring) as the network and systems in school and therefore staff are responsible for risk assessing and managing

such situations. Staff should seek advice from the DSL where necessary.

## 19. Searching and confiscation

19.1.1. In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises.

19.1.2. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying. Full details of the school's search procedures are available in the school Behaviour Policy

## 20. Extremism

20.1.1. The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty – for support with this, please visit prevent.lgfl.net ]. Staff must not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be easily accessed and highly prevalent on mainstream platforms.

## 21. CCTV

21.1.1. The school utilises CCTV to ensure the safety and security of our premises. The use of CCTV is balanced with the right to privacy and ensuring dignity is not compromised. Footage is securely stored, access is restricted to authorised personnel only, and all members of our community are made aware of the presence of CCTV in accordance with DfE Guidance on Data Protection and CCTV in schools.

[https://www.inspirewestthornton.co.uk/attachments/download.asp?file=730&type=pdf]

# 1. Appendix A

## 1.1. Roles

1.1.1. Please read the relevant roles & responsibilities section from the following pages. All school staff must read the "All Staff" section as well as any other relevant to specialist roles.

1.1.1.1. All Staff
1.1.1.2. Headteacher/Principal
1.1.1.3. Designated Safeguarding Lead
1.1.1.4. Trustees, Trust Education Leads and Local Community Councils (LCC)
1.1.1.5. PSHE / RHE Lead/s
1.1.1.6. Computing Lead
1.1.1.7. Subject / aspect leaders
1.1.1.8. Network Manager/technician
1.1.1.9. Data Protection Officer (DPO)
1.1.1.10. Volunteers and contractors (including tutor)
1.1.1.11. Pupils
1.1.1.12. Parents/carers
1.1.1.13. External groups including parent associations

### 1.1.2. All staff

1.1.3. All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school's main safeguarding policy, the code of conduct/handbook (https://www.inspirewestthornton.co.uk/information/policies) and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

1.1.4. They must report any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2025) and guidance (such

as KCSIE), modeling safe, responsible and professional behaviors in their own use of technology at school and beyond and avoiding distressing, victim-blaming language.

1.1.5. Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

### 1.1.6. Head Teacher

Key responsibilities:

1.1.6.1. Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.

1.1.6.2. Oversee and support the activities of the designated safeguarding lead team and ensure they work with technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school)

1.1.6.3. Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.

1.1.6.4. Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.

1.1.6.5. Ensure ALL LCC and Trustees (Central responsibility) undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that LCC members and Trustees are regularly updated on the nature and effectiveness of the school's arrangements

1.1.6.6. Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles.

1.1.6.7. Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the DfE standards—through regular

liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.

1.1.6.8. Liaise with the designated safeguarding lead on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.

1.1.6.9. Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and LCC members to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.

1.1.6.10. Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.

1.1.6.11. Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.

1.1.6.12. Ensure the school website meets statutory requirements.

.

### 1.1.7. Designated Safeguarding Lead / Online Safety Lead – Donna Callaghan

#### 1.1.7.1. Key responsibilities (remember the DSL can delegate certain online-safety duties but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education):

1.1.7.1.1. The DSL should "take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place).

1.1.7.1.2. Ensure "An effective whole school approach to online safety as per KCSIE.

1.1.7.1.3. Ensure the school is complying with the DfE's standards on Filtering and Monitoring.

1.1.7.1.4. As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the

relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.stateherewhatyourmode/searchenginesare

1.1.7.1.5. Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. RHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused.

1.1.7.1.6. Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.

1.1.7.1.7. This must include filtering and monitoring and help them to understand their roles.

1.1.7.1.8. All staff must read KCSIE Part 1 and all those working with children also Annex B

1.1.7.1.9. Cascade knowledge of risks and opportunities throughout the organisation

1.1.7.1.10. Ensure ALL LCC and trustees (Central responsibility) undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that LCC members and Trustees are regularly updated on the nature and effectiveness of the school's arrangements

1.1.7.1.11. Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.

1.1.7.1.12. Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.

1.1.7.1.13. Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online-safety and behavior apply.

1.1.7.1.14. Work closely with SLT, staff and technical colleagues to complete an online safety audit (which is part of the annual safeguarding audit completed with the Trust)

1.1.7.1.15. Work with the headteacher, DPO and Trust central team to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.

1.1.7.1.16. Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net

### 1.1.8. Trustees, Trust Education Leads and Local Community Councils (LCC)

1.1.8.1. Receive regular updates in online-safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter

1.1.8.2. Ensure that online-safety education is embedded across the curriculum in line with the statutory RHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life

1.1.8.3. Promote an awareness of and commitment to online-safety throughout the school community, with a strong focus on parents – dedicated resources at parentsafe.lgfl.net.

1.1.8.4. Communicate regularly with SLT and the Central Safeguarding Team monitoring (termly) to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.

1.1.8.5. Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.

1.1.8.6. Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when unwell, e.g. a survey to facilitate disclosures and an online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox

1.1.8.7. Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).

### 1.1.8.8. Key responsibilities:

1.1.8.8.1. Trustees approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board

By doing this the Trust Education Leaders will;

1.1.8.8.2. Undergo (and signpost all other LCCs and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated

1.1.8.8.3. Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated

1.1.8.8.4. Co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL)

1.1.8.8.5. Support the school in encouraging parents and the wider community to become engaged in online safety activities

1.1.8.8.6. Make sure that the school teaches pupils how to keep themselves and others safe, including online.

1.1.8.8.7. Work with the DPO, DSL and headteacher to ensure a compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information

1.1.8.8.8. Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B

1.1.8.8.9. Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring

1.1.8.8.10. "Ensure that children are taught about safeguarding, including online safety…as part of providing a broad and balanced curriculum…
Consider a whole school or college approach to online safety with
a clear policy on the use of mobile technology."

1.1.8.8.11. The Trustees hold Trust Education Leaders to account for ensuring that the schools in the Trust have appropriate filtering and monitoring systems in place on school devices and school networks, and that the effectiveness is regularly reviewed. The Trust Education Leaders will review the DfE's filtering and monitoring standards, and discuss with Trust IT lead and

service providers what needs to be done to support the schools in meeting the standards, which include:

1.1.8.8.12. Identifying and assigning roles and responsibilities to manage filtering and monitoring systems

1.1.8.8.13. Reviewing filtering and monitoring provisions at least annually

1.1.8.8.14. Blocking harmful and inappropriate content without unreasonably impacting teaching and learning

1.1.8.8.15. Having effective monitoring strategies in place that meet the school's safeguarding needs

### 1.1.9. PSHE / RHE Lead - Debbie Scott

#### 1.1.9.1. Key responsibilities:

1.1.9.1.1. As listed in the 'all staff' section, plus:

1.1.9.1.2. With the SLT, share the responsibility for; embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures online into the PSHE / Relationships education, relationships and sex education (RHE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognize and display respectful behavior online. Throughout these subjects, teachers will address online safety and appropriate behavior in an age appropriate way that is relevant to their pupils' lives."

1.1.9.1.3. Focus on the underpinning knowledge and behaviors outlined in Teaching Online Safety in Schools in an age appropriate way

to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.

1.1.9.1.4. Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RHE.

1.1.9.1.5. Note that an RHE policy should be included on the school website.

1.1.9.1.6. Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

### 1.1.10. Computing Lead - Mohamed Kamara

#### 1.1.10.1. Key responsibilities: As listed in the 'all staff' section, plus:

1.1.10.1.1. Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum

1.1.10.1.2. Work closely with the RHE lead to avoid overlap but ensure a complementary whole-school approach

1.1.10.1.3. Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

1.1.10.1.4. Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

### 1.1.11. Subject leaders

#### 1.1.11.1. Key responsibilities as listed in the 'all staff' section, plus:

1.1.11.1.1. Look for opportunities to embed online safety in your subject or aspect, especially as part of the RHE curriculum, and model positive attitudes and approaches to staff and pupils alike

1.1.11.1.2. Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context (this is covered in the IPAT curriculum).

1.1.11.1.3. Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

1.1.11.1.4. Ensure subject specific action plans also have an online-safety element.

### 1.1.12. Network Manager/other technical support roles - Turn IT On

#### 1.1.12.1. Key responsibilities as listed in the 'all staff' section, plus:

1.1.12.1.1. Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.

1.1.12.1.2. Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks.

1.1.12.1.3. Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.

1.1.12.1.4. Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

1.1.12.1.5. Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.

1.1.12.1.6. Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.

1.1.12.1.7. Maintain up-to-date documentation of the school's online security and technical procedures.

1.1.12.1.8. To report online-safety related issues that come to their attention in line with school policy.

1.1.12.1.9. Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.

1.1.12.1.10. Ensure the data protection policy is up to date, easy to follow and practicable.

1.1.12.1.11. Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.

### 1.1.13. Data Protection Officer (DPO) - Stephen Schwartz / DPO centre

#### 1.1.13.1. Key responsibilities:

1.1.13.1.1. Alongside those of other staff, provide data protection expertise and training and support the Data Protection policy

and compliance with those and legislation and ensure that the policies conform with each other and with this policy.

1.1.13.1.2. Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in data protection in schools, 2023, “It’s not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child.” And in KCSIE 2025, “The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.”

1.1.13.1.3. Note that retention schedules for safeguarding records may be required to be set as ‘Very long-term need (until pupil is aged 25 or older)’. However, some local authorities require record retention until 25 for all pupil records. You should check the requirements in your area.

1.1.13.1.4. Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

### 1.1.14. Volunteers and contractors (including tutors)

#### 1.1.14.1. Key responsibilities:

1.1.14.1.1. Read, understand, sign and adhere to an acceptable use policy (AUP)

1.1.14.1.2. Report any concerns, no matter how small, to the designated safety lead

1.1.14.1.3. Maintain an awareness of current online safety issues and guidance

1.1.14.1.4. Model safe, responsible and professional behaviors in their own use of technology at school and as part of remote teaching or any online communications

1.1.14.1.5. Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

### 1.1.15. Pupils

#### 1.1.15.1. Key responsibilities:

1.1.15.1.1. Read, understand, sign and adhere to the student/pupil acceptable use policy

### 1.1.16. Parents/carers

#### 1.1.16.1. Key responsibilities:

1.1.16.1.1. Read, sign and adhere to the school's parental acceptable use policy (AUP), read the pupil AUP and encourage their children to follow it

### 1.1.17. External groups including parent associations

1.1.17.1. Key responsibilities:

1.1.17.1.1. Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school

1.1.17.1.2. Support the school in promoting online safety and data protection

1.1.17.1.3. Model safe, responsible, respectful and positive behaviors in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, LCC members, contractors, pupils or other parents/carers

# 2. Appendix B: The National Landscape of Online Safety

2.1.1. Nationally, some of the latest trends of the past twelve months are outlined below. These are reflected in this policy and the acceptable use agreements we use and see in the context of the 4 Cs (see KCSIE for more details).

## 2.2. National Online Safeguarding Trends

.

2.2.1. LGFL SENSO MONITORING

2.2.1.1. The following are concerns highlighted through LGfL's partnership with Senso and monitoring data from LGfL schools. Many children are using Gen AI platforms on the school network and/or school devices, and the following have occurred:

2.2.1.2. The creation of child sexual abuse material by and of children

2.2.1.3. The spread of AI generated hoaxes, misinformation and disinformation. Sometimes these can be so realistic that it is difficult to determine what is true or not. One notable example of this was the sharing of fake information across social media about serious threats of violence in and between schools, which led to children/parents being fearful and some not attending school.

2.2.1.4. Children turning to Gen AI platforms for advice – some of which is harmful and extremely worrying, e.g. dieting, relationships, bullying, and advice about self-harm

2.2.1.5. Increased use of AI companions and chatbots which mimic human connection and have been seen to lead to AI induced psychosis, overuse, and heightened feelings of loneliness and shame. Tragically, there have also been numerous cases worldwide of children dying by suicide as a result of interactions with such bots.

2.2.1.6. There have also been numerous concerns related to staff use of Gen AI, including privacy and intellectual property breaches, and an increase in poor quality learning resources created using Gen AI.

2.2.1.7. Schools must address this, not just in the classroom, but by educating staff, governors, trustees, parents and pupils on safe use of digital technology, both for school and personal use. For guidance and resources, visit genai.lgfl.net.

### 2.2.2. LGfL Senso monitoring data has also revealed other concerns in schools:

2.2.2.1. Children accessing inappropriate online games, dating sites and web chat where there is the risk of seeing adult and violent content and having interactions with strangers.

2.2.2.2. The normalisation of violent and racist language between children, much of which doesn't suggest a particular ideology, but which could lead to extremism.

2.2.2.3. All these issues require a whole school approach to online safeguarding, as there is no quick or simple solution. It requires a combination of strong leadership, clear roles and responsibilities, robust policies and procedures, effective technical systems, highly competent staff who are regularly updated on this fast-paced world, effective and regular collaboration with parents, successful digital literacy and online safety teaching and more.

## 2.3. OFCOM'S LATEST RESEARCH

2.3.1. Ofcom's 'Children and Parents media use and attitudes report' published in 2026 has shown the following:

2.3.1.1. Internet use is nearly universal, with 99% of 8-17-year-olds going online, and the vast majority of children are using digital technology by the time they start primary school. A critical transition occurs at age 11, where personal mobile phone ownership jumps from 56% to 83%. Schools must also address the rapid adoption of Generative AI, now used by 56% of 8-17-year-olds, primarily for schoolwork (51%). Despite high confidence, a 'digital literacy gap' exists: 31% of students could not identify a fake social media profile, and 46% believe AI search summaries are "always accurate".

2.3.1.2. Social pressures remain high, with 70% of students feeling pressure to be popular on social apps. Negative experiences are common; 23% of 8–17-year-olds personally experienced "nasty or hurtful" behaviour in the last year, occurring most frequently on social media (47%) and in online games (38%). Vulnerable students, such as those with mental health conditions, are significantly more likely to feel their screen time is "too high" (56%).

2.3.1.3. Schools are the primary source of online safety information for 49% of parents. While 85% of students recall online safety lessons, only 23% remember being taught how to spot AI-generated content, and 21% recall lessons on identifying advertising. This suggests a need for updated curricula that reflect the evolving risks of AI and commercial influence.

## 2.4. IWF, CSAM CONCERNS

2.4.1. Data from the IWF in their 2025 annual report highlights the scale of child sexual abuse imagery online. In 2025, the IWF assessed 451,210 reports, confirming that 311,610 contained child sexual abuse material (CSAM).

2.4.2. Schools should be specifically alert to emerging and persistent harms identified by the IWF, which include:

2.4.3. Sexually coerced extortion (sextortion): Targeted threats against students – teenage boys in particular.

2.4.4. AI-generated abuse: The use of generative tools to create non-consensual sexual imagery.

2.4.5. Violence against women and girls (VAWG): A growing trend in digital spaces around violent and misogynistic narratives and language.

## 2.5. “COM NETWORKS”

2.5.1. A further concern highlighted by the National Crime Agency, is that of the existence of ‘Com Networks’. These are networks of predominantly teenage boys, dedicated to inflicting harm and committing a range of criminality both

on and offline, including cyber, fraud, extremism, serious violence, and child sexual abuse. The victims of these crimes are typically other children, some as young as 11, who have been coerced into seriously harming or sexually abusing themselves, siblings or pets. These networks are not hidden away in the dark web, but instead on platforms such as Discord, Telegram, Roblox, and Minecraft. Schools can help to protect children from these networks by enforcing effective filtering, training staff to recognise signs of exploitation, supporting parents to understand and mitigate the risks and building a curriculum that teaches students to identify grooming behaviours.

## 2.6. CYBER ATTACKS

2.6.1. Data from the Department for Science, Innovation and Technology (DSIT) states that 73% of secondary schools and 49% of primary schools identified a cyber breach or attack in the past 12 months (a significant jump from the previous year). Phishing remains the biggest entry point. AI is being used by scammers to generate sophisticated, error-free phishing emails targeting school administration and staff accounts. Schools are encouraged to ensure that they bridge the gap between technical understanding/cyber security policies, and operational understanding and practice.

.