DIOCESE OF CHICHESTER ACADEMY TRUST

ONLINE SAFETY POLICY

Date Agreed:	**September 2026**
Review Date:	**September 2027**
Type of Policy:	**DCAT Statutory Policy**

Revision Number	Date Issued	Prepared by	Approved	Personalised by school	Comments
2	September 2026	SWGfL Reviewed by DI/MM	Trust Board		Trust policy to be personalised by all schools
1	February 2024	SWGfL	Trust Board		SWGfL policy to be personalised by all schools

Type of Policy	*Tick* ✓
DCAT Statutory Policy	✓
DCAT Non-statutory Policy	
DCAT Model Optional Policy	
Academy Policy	
Local Authority Policy	

Northiam Primary School

Contents

1. Policy Aims 2
2. Policy development, monitoring and review 2
3. Policy and leadership 2
   - Headteacher and senior leaders 3
   - Governors 3
   - Designated Safeguarding Lead (DSL) 4
   - Online Safety Lead (OSL) 4
   - Curriculum Leads 4
   - Teaching and Support Staff 4
   - IT service provider / technical staff 5
   - Learners 5
   - Parents and carers 5
   - Community users 5
4. Online Safety Group 6
5. Policy 6
6. Acceptable use 7
7. Reporting and responding 10
8. Use of Artificial Intelligence (AI) 16
9. Education 17
10. Staff 18
11. Governors 19
12. External Stakeholders 19
13. Technology 21
    - Filtering and Monitoring 21
    - Technical Security 21
    - Cyber Security 22
    - Data Protection 22
14. Technology Practice 23
    - Device Management 23
    - Digital Content 23
    - Public Online Communications 24
15. Outcomes 24
16. List of appendices 25

Appendix A1- Learner Acceptable Use Agreement Template – for older learners 26

Appendix A2 - Acceptable Use Agreement Template – for KS2 Learners 28

Appendix A3 - Acceptable Use Agreement Template – for younger learners (EY/KS1) 30

Appendix A4 - Parent/Carer Acceptable Use Agreement Template 31

Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement Template 35
Appendix A6 - Acceptable Use Agreement for Community Users Template 38
Appendix A7 - Online Safety Policy Statement 39
Appendix A8 Responding to incidents of misuse – flow chart 42
Legislation 1
Links to other organisations or documents 6

Introduction

Our **vision** for our Trust is we exist to:

Help every child achieve their God-given potential

Our **aims** are clear. We aim to be a Trust in which:

Developing the whole child means pupils achieve and maximise their potential

Continued development of staff is valued and improves education for young people

All schools are improving and perform above national expectations

The distinct Christian identity of each academy develops and is celebrated

Our work as a Trust is underpinned by shared **values**. They are taken from the Church of England's vision for Education and guide the work of Trust Centre team. They are:

Aspiration
I can do all things through Christ who strengthens me
(Philippians 4 vs 13).

Wisdom
Listen to advice and accept discipline, and at the end you will be counted among the wise
(Proverbs 19 vs 20)

Respect
So in everything do to others what you would have them do to you
(Matthew 7 vs 12)

Our vision of helping every child achieve their God-given potential is aligned with the Church of England's vision for education and is underpinned by the Bible verse from John: *I have come that they may have life, and have it to the full.*

Guidance notes for schools that must be deleted prior to publishing your completed policy.

This is a Trust policy that needs to be personalised where indicated where highlighted in yellow prior to publication. Blue writing indicates guidance notes throughout the policy and should also be deleted prior to publication. An effective Online Safety Policy must be tailored to the needs of each school and personalisation sections should reflect practice in your school.

Schools must review their Online Safety Policy at least annually, (KCSIE Para 121) and more frequently where there are significant changes in technology, risks, or technology-related behaviours. The policy should be available publicly either via the school website or by other means.

Keeping Children Safe in Education (KCSIE) requires Local Authorities, Multi-Academy Trusts and schools to ensure children are safeguarded from harmful and inappropriate online material, and that online safety is a running and interrelated theme across the whole-school safeguarding approach. This includes how online safety is reflected in relevant policies, the curriculum, staff training, the role of the DSL (and deputies), and parental engagement. KCSIE also recommends an annual review supported by a risk assessment; schools should use the 360 safe self-review tool to support this process.

KCSIE (Para 163 – updated July 2026) describes online safety risks across four broad areas:

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,
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
3. **Conduct**: behaviour that increases likelihood of harm for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
4. **Commerce:** risks such as gambling, inappropriate advertising, phishing and financial scams.

Schools in England are subject to increased scrutiny of online safety through inspection, and the Counter Terrorism and Security Act 2015 requires schools to protect learners from terrorist and extremist material online.

1. Policy Aims

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and community users**.** It applies to use of school systems both on and off site**,** and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, Northiam Primary School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

2. Policy development, monitoring and review

This policy has been developed by the DSLs drawing on the expertise and responsibilities across the school. Membership includes: (amend as appropriate)

- Headteacher / Senior leaders
- Designated Safeguarding Lead (DSL)
- Online Safety Lead (OSL)
- Staff (including teaching, support and technical staff)
- Governors
- Parents/carers
- Community users (where relevant)

Escalation following serious incidents: the school will inform relevant external agencies as appropriate.

Named contacts/agencies: DCAT Head of Safeguarding, LADO and/or the Police.

Monitoring the impact of the policy

The school will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Reviews of the effectiveness of the filtering systems
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Learners, Parents/carers, Staff

3. Policy and leadership

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.
Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Establish a nominated SLT Lead to work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded

Governors

Governors approve the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated
- Ensure that children be taught about safeguarding, including in relation to online safety
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

The governing body will nominate an Online Safety Governor who will:

- Meet regularly with the DSL/OSL.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the relevant governor group/committee**:** Julia Bray, Sam Mewett, Katie Babicz
- Undertake basic cyber security awareness training and support school cyber security oversight.
- Participate in the Online Safety Group (where in place).

Governors also support parent/carer and community engagement in online safety.

Designated Safeguarding Lead (DSL)

KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to explicit in the DSL's job description.

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information.
- With the nominated SLT Lead and the IT provider lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for learners with SEND.

Online Safety Lead (OSL)

The OSL will:

- Lead the Online Safety Group and support the DSL day to day.
- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Curriculum Leads

Curriculum leads will work with the DSL/OSL to deliver a planned online safety programme (e.g. ProjectEVOLVE) through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture. Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.

- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

IT service provider / technical staff

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to Sam Mewett
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Learners

Learners will:

- Follow the Learner AUA and Online Safety Policy (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy and share the learner AUA
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

Community users

Community users accessing school systems or platforms will sign a Community User AUA before access is provided. The school welcomes partnership working and shares good practice where appropriate.

4. Online Safety Group

The Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice. In some schools it may sit within a wider safeguarding or digital strategy group.

Membership

- DSL, OSL, Senior Leader(s)
- Safeguarding Link Governor
- IT/technical representative (internal or provider)
- Staff representatives (teaching/support)
- Learner representative(s)
- Parent/carer representative(s)
- Community/external partner (where relevant)

Core responsibilities

The group supports the DSL/OSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Gather feedback from learners, staff and parents/carers and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.
- Track and evidence improvement actions (e.g. 360 safe).

Governance and impact

- Operates to agreed Terms of Reference (membership, frequency, reporting lines), reviewed annually.
- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Learner Voice as needed.
- Reports key themes, actions and impact to SLT and governors, and shares appropriate summaries with the wider community.

5. Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside the Child Protection and Safeguarding, Behaviour, Anti-Bullying and Data Protection policies.

What the policy does

- Defines responsibilities for online safety.
- Sets expectations for safe, professional and ethical use of technology (including AI).
- Sets out reporting, recording and response procedures for online safety incidents.
- Supports compliance with KCSIE, DfE Technical Standards and UK GDPR.
- Promotes learners' digital competence and critical understanding.

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually (KCSIE Para 121), and sooner if risks/technology change.

- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. 360 safe, ProjectEVOLVE).
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training.
- Communicated to learners and parents/carers through AUAs and awareness activity.
- Published on the school website.

6. Acceptable use

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs). AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

- staff and learner induction/handbooks
- on-screen reminders (e.g. splash screens), digital signage
- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- school website
- peer support / learner-led activity

Acceptable/Unacceptable Actions

Schools should agree what is acceptable/unacceptable for their context (age, setting and systems) and record this in the tables below.

User actions		**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable & illegal**
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	• Fraud and financial crime (including money laundering) • *Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).*					
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts) • Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (e.g., denial of service) • Using penetration-testing tools without explicit permission *Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime* and into positive pathways.					X
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (*e.g. Roblox, Fortnite, Minecraft*)	X				X			
Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)*	X				X			
Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*)		X			X			
Social media and user-generated platforms *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services*	X				X			
Messaging, chat and voice *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)*	X				X			
Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify*	X				X			
Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)*		X			X			
Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds). N.b Smartphone bans in schools in England)*			X		X			

Taking photos/video/audio on devices (including sharing, location data and consent)		X					X	
Other personal devices *(e.g., tablets, handheld consoles, VR headsets, wearables)*		X			X			
Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)*			X		X			
School email used for personal communication (non-work/non-learning)		X			X			
Unapproved AI tools/services *(generative AI chatbots and image/video tools, AI companions, browser extensions)*								

7. Reporting and responding

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Children Safe in Education (KCSIE)*, the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The school recognises national findings, including the Ofsted *Review of Sexual Abuse in Schools and Colleges* (2021), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child.

Reporting Concerns
The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns
The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.

- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring

The school will:

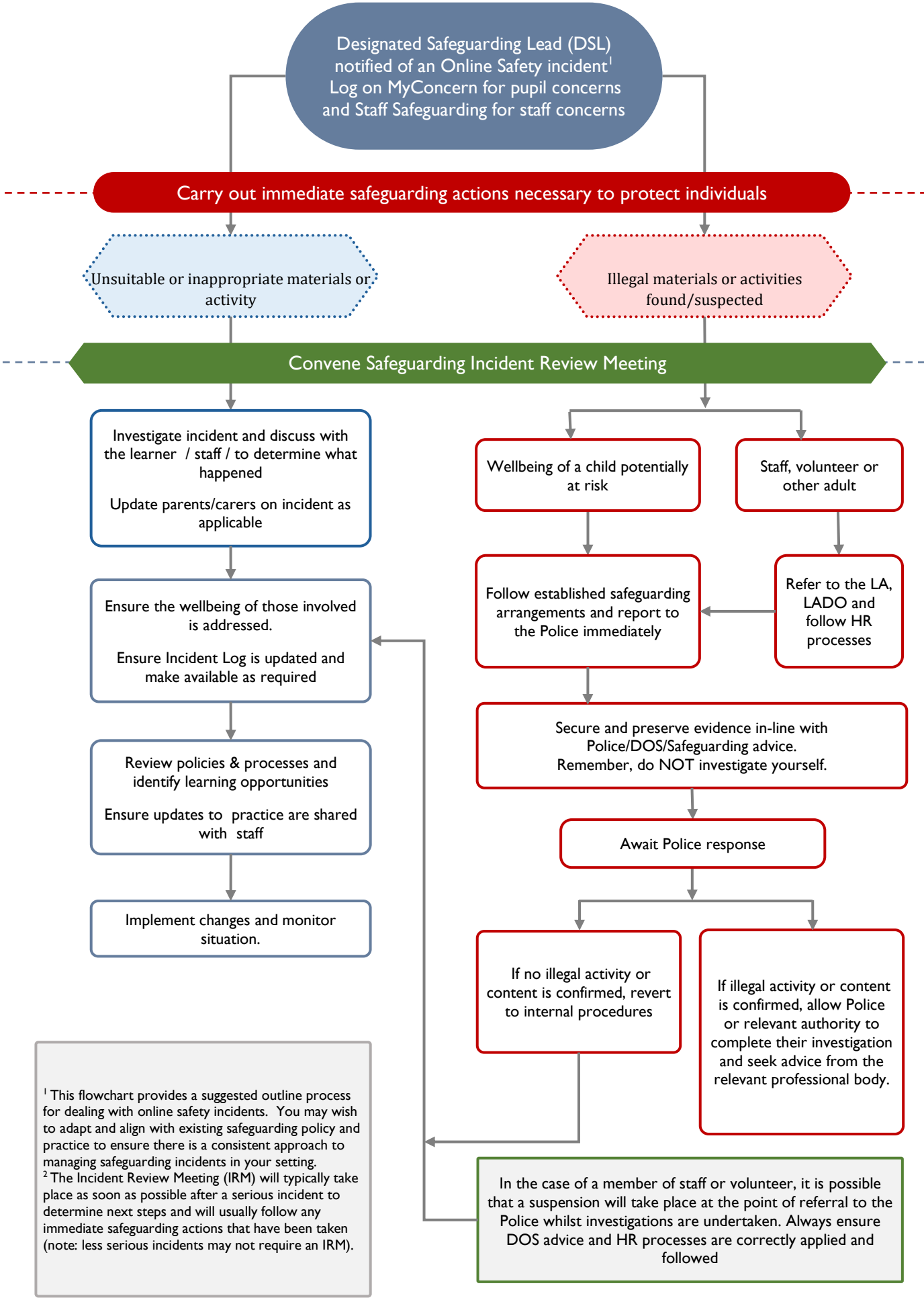
- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
    - The Online Safety Group
    - Senior leaders
    - Governors (via safeguarding reports)
    - *Staff*
    - *Learners, where appropriate*
    - *Parents/carers through general communications*
    - *Local safeguarding partners where relevant*

External Support and Escalation

Schools should consult with the Trust Head of Safeguarding regarding any high-risk online activity as soon as possible.

The school will work with the Trust Head of Safeguarding and appropriate external agencies when required, including:

- Local Authority safeguarding teams
- Local Authority Designated Officer (LADO)
- Police / CEOP
- Local Safeguarding Partnership guidance (e.g., harmful sexual behaviour support)
- UK Safer Internet Centre's Professionals Online Safety Helpline
- Reporting Harmful Content service


Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]
Log on MyConcern for pupil concerns and Staff Safeguarding for staff concerns
Carry out immediate safeguarding actions necessary to protect individuals
Unsuitable or inappropriate materials or activity
Illegal materials or activities found/suspected
Convene Safeguarding Incident Review Meeting
Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable
Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required
Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff
Implement changes and monitor situation.
Wellbeing of a child potentially at risk
Staff, volunteer or other adult
Follow established safeguarding arrangements and report to the Police immediately
Refer to the LA, LADO and follow HR processes
Secure and preserve evidence in-line with Police/DOS/Safeguarding advice.
Remember, do NOT investigate yourself.
Await Police response
If no illegal activity or content is confirmed, revert to internal procedures
If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed
[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to DSL / OSL	Refer to SLT	Refer to Trust Head of Safeguarding	Refer to Police/Social Services	Refer to IT Services Provider	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X	X					
Unauthorised access to the school network, including using another person's account or sharing usernames/passwords.		X	X	X			X		X	
Damaging, corrupting or deleting another user's data.				X					X	
Sending offensive, harassing or bullying emails, texts or messages.		X	X	X	X		X		X	
Unauthorised downloading/uploading, file sharing or distribution of files.		X	X				X		X	
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).		X	X							
Failing to report accidental access to offensive or pornographic material		X	X	X	X	X	X	X	X	
Deliberately accessing offensive or pornographic material (or attempting to)		X	X	X	X	X	X	X	X	
Sharing or receiving content that breaches copyright or data protection law.		X	X	X	X	X	X	X	X	
Unauthorised use of devices, including taking photos/videos or audio recordings and using a smartphone in school		X	X	X	X	X	X	X	X	
Unauthorised use of online services (apps, websites or platforms). N.b. this may need to be updated in		X	X	X	X	X	X	X	X	

response to the projected social media ban for U16s.										
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.		X	X	X	X		X	X	X	
Repeated breaches of these rules following previous warnings or sanctions.		X	X	X	X		X	X	X	

Incidents	Refer to line manager	Refer to SLT / Headteacher	Refer to Trust Head of Safeguarding	Refer to Police / LADO	Refer to IT Services Provider	Issue a warning	Further Disciplinary action in line with Behaviour Policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X			
Breaching data protection or cyber-security requirements, including network security rules.		X	X	X	X		
Accessing offensive or pornographic material (or attempting to).	X	X	X	X	X		X
Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software.	X	X	X		X	X	X
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).	X	X	X				x
Unauthorised downloading, uploading or file sharing.		x	x				
Breaching copyright, licensing or intellectual property, including misuse of AI systems.	X	X	X				x
Unauthorised account/network access, including sharing passwords, using another person's account, or allowing others access.							
Sending offensive, harassing or bullying emails, texts or messages.	X	X	X		X	X	X
Use of personal email/social media/messaging to communicate with learners or parents/carers.						x	
Inappropriate personal use of school technology, including personal email and social media use during work time/using school systems.						x	
Mishandling personal data, including storing, displaying or transferring it insecurely.		x	x				
Any action that undermines professional conduct or a staff member's professional standing.		X	X	X			
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X				

Failing to report incidents, whether accidental or deliberate.		x	x			x	
Repeated breaches following previous warnings or sanctions.	x	x	x				x

8. Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

The school will:

- Follow guidance within the DCAT AI Guidelines.
- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

- Protect personal and sensitive data.
  Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance.
  Staff must ensure any AI tool used meets data protection and security requirements before use and request a Data Protection Impact Assessment (DPIA) from the AI provider and forward to the Trust for approval. See DCAT AI Guidelines for full details.
- Approve tools and accounts.
  Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information.
  Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, for pupil concerns report to your Designated Safeguarding Lead and follow the usual staff safeguarding procedures for staff related incidents.
- Trust will maintain an inventory of AI tools in use across the Trust.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support learners in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the DCAT Disciplinary Policy.

9. Education

Online Safety Education Programme

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including DfE "Teaching Online Safety in Schools", UKCIS "Education for a Connected World", and resources such as SWGfL ProjectEVOLVE). Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing

curriculum areas (including RSHE/RSE, Health Education, Computing and Citizenship), with assessment and clear intended outcomes.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation (e.g. on an Online Safety Group), and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

10. Staff

In line with DfE Keeping Children Safe in Education (KCSIE), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include (select/delete as appropriate):
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- staff understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
- staff understand that filtering and monitoring supports - but does not replace - effective supervision, professional curiosity and safeguarding judgement

- staff are informed of the outcome of the school's annual filtering and monitoring review where relevant to their roles
- staff understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices. They know how authorised exceptions for learners are approved and managed.
- staff follow cyber security policy and requirements.
- Online safety training is provided for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Lead and Online Safety Lead (or other nominated staff) through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources (e.g. ProjectEVOLVE EDU) and, where appropriate, enhanced pathways (e.g. ProjectEVOLVE SAFEGUARDING).
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL/OSL (or nominated staff) to individuals as required.

11. Governors

Governors should take part in online safety training and awareness activity. This is particularly important for governors serving on committees with responsibility for safeguarding, online safety, technology or health and safety.

Training and updates may be provided through

- Attendance at training offered by the Trust.
- Participation in school training and information sessions (for example, staff briefings or parent events). This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

Enhanced training will be provided for (at least) the Online Safety Governor. This will include:

- Basic cyber security awareness training.
- Training to understand the school's filtering and monitoring provision, enabling effective participation in required checks and reviews.

12. External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

Working with Parents and Carers

The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources (e.g. UK Safer Internet Centre, Internet Matters, Childnet, SWGfL).
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.
- clear communication about the school's mobile-phone arrangements, the reasons for the policy, authorised exceptions and the consequences of breaches
- accurate, balanced and age-appropriate information about changes affecting social media and other online services
- guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

The school recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.

- Supporting external groups to review and improve their own online safety practice, including through recommended tools such as 360 Early Years or 360 Groups.

13. Technology

The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider school community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., DfE Technical Standards, DfE Generative AI: product safety standards; KCSIE) and best practice guidance (e.g., UKSIC Appropriate Filtering and Monitoring). The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content

Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities
- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Testfiltering). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. (KCSIE 2026 refers to the DfE Cyber Security Standards and recognises cyber security as a safeguarding issue).

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and their safeguarding implications receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Refer to the DCAT Cyber Incident Response Plan.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation. (The Data (Use and Access) Act 2025 makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards).

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

Further detail is provided in the DCAT Data Protection Policy.

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

14. Technology Practice

The school recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in *Keeping Children Safe in Education*, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice, education and staff training. It also supports the DfE digital and technology standards and the school's responsibilities for filtering, monitoring, cyber security and digital leadership.

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education.

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education
- learners do not have access to mobile phones or other personal smart devices throughout the school day, in accordance with the school's Behaviour and Mobile Phone policies (in line with the DfE statutory guidance)
- any exceptions are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or SEND-related reasons
- staff model the school's requirements and use personal devices only where authorised and professionally appropriate
- procedures cover possession, storage, confiscation, searching and return of devices, in accordance with school policy and current national guidance.

Decisions about device use are informed by risk assessment and reviewed regularly.

Digital Content

The school recognises that multi-modal digital content (inc. AI) can enrich learning and communication when used responsibly. Its approach supports safeguarding requirements in particular, sexual imagery, consent, coercion, privacy and the sharing or manipulation of content.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently

- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- school-approved platforms and accounts are used where content includes personal or sensitive information
- staff and learners understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on Protecting your setting's images from AI manipulation and abuse.

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (guidance is available from UKSIC)
- publishing public communications is restricted to authorised and trained staff
- AI-assisted public communications are checked by an authorised person before publication and remain subject to human accountability. AI assisted content should be clearly labelled as such.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, learners and parents
- national guidance and statutory expectations
- the school's progress towards meeting the DfE digital and technology standards
- the impact of mobile-phone arrangements and changes affecting children's access to online services.

15. Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, learners and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's

assessment processes (e.g. using ProjectEVOLVE Knowledge Maps assessment and tracking). Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety

16. List of appendices

A1 - Learner Acceptable Use Agreement Template – for older learners
A2 - Learner Acceptable Use Agreement Template – KS2
A3 - Learner Acceptable Use Agreement Template – for younger learners (EY/KS1)
A4 - Parent/Carer Acceptable Use Agreement Template
A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
A6 - Community Users Acceptable Use Agreement Template
A7 – Online Safety Policy Statement Template
A8 - Responding to incidents of misuse – flow chart
Legislation
Links to other organisations and resources

Appendix A1- Learner Acceptable Use Agreement Template – for older learners

Learner Acceptable Use Agreement Form

I agree to use the school's digital systems, devices and online services responsibly to protect my safety, the security of the school systems, and others.

Personal Safety

- The school will monitor my use of its digital systems, devices, online services and communications.
- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.
- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I understand that images and videos can be copied, altered (including using AI) and shared beyond my control.
- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.

Respecting Others' Work and Information

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.
- I will only use Artificial Intelligence (AI) tools approved by the school and ensure my use is ethical, legal, and transparent.
- When I use generative AI to assist in creating digital content, I will ensure it is labelled as such.
- I will check AI-generated content carefully, recognising that it may be inaccurate, misleading or biased, before using or sharing it.
- I will fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- I will avoid downloading or using copyrighted or protected materials without proper permissions.

Responsible Online Behaviour

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not bully, harass, threaten, upset or make fun of others.
- I will only use platforms or software approved by the school and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand cybersecurity poses a risk to both me, other learners and the school and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.

- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the school's requirements for using mobile phones and other connected devices.
- I understand that age restrictions are designed to help protect children and young people. If I use online services, I will do so safely, responsibly and in accordance with school requirements.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of the school, its staff, and other learners.
- I will ensure my behaviour reflects positively on the school, both in and out of school settings.
- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, learners in embarrassing situations or the setting up of fake accounts.
- I know I can talk to a trusted adult if I am worried about anything I see or experience online, even if I think I may have broken one of these rules.

Consequences of Misuse

- I understand that failing to follow this agreement may lead to consequences, including loss of access to the school's systems, detentions, suspensions, contacting parents/carers, or involvement of the police in serious cases.

By following these guidelines, I will contribute to a safe, respectful, and productive online environment.
I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed)
- I use digital technologies out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Name of Learner: ..... Group/Class: .....
Signed: ..... Date: .....

Parent/Carer Countersignature

Appendix A2 - Acceptable Use Agreement Template – for KS2 Learners

Acceptable Use Agreement
I agree to use the school's digital systems, devices and online services safely and responsibly to protect me, other learners and the school.

Keeping Safe Online

- The school will check how I use devices and online services to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Devices and Online Services Sensibly

- I will only use devices, apps, games and websites that my teacher or parent/carer says are suitable for my age.
- I know that I am not allowed to use some online services and I know what they are.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I understand that not every app or website is suitable for children my age.
- If I want to join a new app, game or online community, I will speak to a trusted adult first.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.
- If I make a mistake online, I know I can ask a trusted adult for help

What Happens If I Break These Rules?

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.
I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)

- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature (optional)

Appendix A3 - Acceptable Use Agreement Template – for younger learners (EY/KS1)

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school. These rules help us all stay safe and have fun using computers and tablets at school!

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.
- I will only use apps and games that a trusted adult says are right for me.
- If I want to try a new game or app, I will ask a trusted adult first.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

Signed (child): ..... Signed (parent): .....

Appendix A4 - Parent/Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at school.

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using devices.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of digital technologies at home and will inform the school if I have concerns over my child's online safety.

This form (electronic or printed)
Who will have access to this form.

Where this form will be stored.
How long this form will be stored for.
How this form will be destroyed.

Signed: .....
Date: .....

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's **delete as relevant** first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such e.g., Social Media, website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored and for how long
How this form will be destroyed.	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital/Video Images Permission Form

Parent/Carers Name:..... Learner Name:.....

As the parent/carer of the above learner, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No

• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
Insert statements here that explicitly detail where images are published by the schools	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: .....
Date: .....

Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for learners.
Schools will need to review and amend the section below, depending on which cloud hosted services are used.
The school uses **insert cloud service provider name** for learners and staff. This permission form describes the tools and learner responsibilities for using these services.

The following services are available to each learner as part of the school's online presence in **insert cloud service provider name**

Using **insert cloud service provider name** will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other learners and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.
As the school is collecting personal data and sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared and with whom
Where this form / data will be stored.	Who will have access to the data.
How long this form will be stored for.	Where the data will be stored and for how long
How this form will be destroyed.	How a request for deletion of the data can be made.

Do you consent to your child to having access to cloud services? Yes/No

Learner Name: ..... Parent/Carers Name: .....
Signed: ..... Date: .....

Use of Biometric Systems in England and Wales

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" and Data Protection legislation) seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual children in the following ways
Biometric technologies have certain advantages over other automatic identification systems as learners do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. Meaning that it is not possible, for example, to recreate a learner's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

As the school is collecting special category personal data and **delete as appropriate** sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared and with whom
Where this form / data will be stored.	Who will have access to the data.
How long this form will be stored for.	Where the data will be stored and for how long
How this form / the data will be destroyed.	How consent to process the biometric data can be withdrawn.

Parent/Carers Name: .....
Learner Name: .....

As the parent/carer of the above learner, I agree to the school using biometric recognition systems, as described above.	Yes/No
I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school.	Yes/No

Signed: .....

Further guidance

- (In England) Each parent of the child should be notified by the school that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school to process children's biometrics at least one parent must consent and no parent has withdrawn consent. This needs to be in writing.
- The child can object or refuse to participate in the processing of their biometric data regardless of parents' consent.
- Schools must provide reasonable alternative means of accessing services for those learners who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the learner attends the school, but new permission is required if there are changes to the biometric systems in use.

Learner Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.
It is suggested that when the learner AUA is written that a copy should be attached to the parents/carers acceptable use agreement to provide information for parents and carers about the rules and behaviours that learners have committed to by signing the form.

Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement Template

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies.

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should always have an entitlement to safe access to the internet and digital technologies.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible, informed and professionally competent users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that filtering and monitoring are safeguarding measures designed to protect learners, staff and school systems. Where my role requires it, I will act promptly on concerns or alerts in accordance with the school's safeguarding procedures.
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any safeguarding, cyber security, filtering, monitoring or data protection concern using the school's agreed reporting procedures.
- I will complete the online safety, safeguarding and cyber security training required by the school and keep my knowledge up to date.

Protecting Learners, School Systems and Information:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will only communicate with learners, parents/carers and colleagues using school-approved systems. Any such communication will be professional in tone and manner
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
  - will only use AI technologies approved by the school
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
  - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
  - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
  - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
  - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
  - I recognise that AI supports, but does not replace, my professional judgement. I remain responsible for the accuracy, appropriateness and safeguarding implications of any AI-assisted work.
- I will follow the school's expectations for the professional use of mobile phones and other connected devices, ensuring only permitted use
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will protect school systems by following the Trust's cyber security procedures.

- I will not access illegal, inappropriate or harmful content on school systems.
- I will respect filtering, monitoring and other security measures and report any concerns about their effectiveness.
- I understand that some websites or services may be restricted for safeguarding reasons and will use the school's agreed process where access is required for legitimate educational purposes.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will only use school-approved cloud services and digital platforms for storing or sharing school information.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using digital technologies in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that my professional responsibilities extend to my conduct in public online spaces where this could affect learners, colleagues or the reputation of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I will model safe, responsible and balanced use of digital technology in my professional practice.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action in accordance with the DCAT Disciplinary Policy.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....
Signed: .....
Date: .....

Appendix A6 - Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

As the school is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form.	How this form will be destroyed.
Where this form will be stored.	How long this form will be stored for.

Name: ..... Signed: ..... Date: ……..

Appendix A7 - Online Safety Policy Statement

At Northiam Primary School we want every user to be safe, confident and supported when using technology - whether learning in school, at home, or in the wider community. Online safety is part of safeguarding and wellbeing. It is not "just an IT issue": it is about people, relationships, behaviour, learning, and protection.
Our online safety strategy is built around four outcomes-focused areas that strengthen day-to-day practice:

- Leadership and policy that make expectations clear
- Education that builds skills, resilience and positive behaviour
- Technology that protects users and supports safe learning
- Impact review that proves what's working and what we will improve

Leadership and policy: clarity, consistency and accountability

- When leadership is strong, online safety becomes part of "how we do things here"—not a one-off initiative.

Clear responsibilities

- We make sure roles are defined and understood across senior leaders, the Designated Safety Lead, an Online Safety Lead, governors/trustees and technical staff/providers. This ensures safeguarding decisions and technical safeguards work together.
- What this improves: decisions are quicker, concerns are escalated correctly, and actions don't get "lost" between teams.
- Benefit for users: children and adults get safer, more consistent support.

A joined-up Online Safety Group

- We involve the right voices—leaders, staff, governors, and (where appropriate) learners and families—to keep online safety responsive to real experiences and emerging risks.
- What this improves: shared ownership and a whole-school approach.
- Benefit for users: safer practice is reinforced across school and home.

A policy that is understood and used

- Our online safety policy is aligned with safeguarding expectations and linked to related policies so that staff and families can see one clear, consistent approach.
- What this improves: fewer grey areas and more confident decision-making.
- Benefit for users: clear boundaries and predictable responses.

Acceptable use expectations that protect everyone

- We set out simple, age-appropriate expectations for learners and clear professional expectations for staff, so everyone understands what safe and respectful use looks like.
- What this improves: behaviour, consistency, and fairness.
- Benefit for users: safer online spaces and fewer harmful incidents.

Reporting and responding that leads to action

- We promote a culture where people feel able to speak up, and we respond consistently, recording concerns, acting promptly, and learning from patterns and new risks.
- What this improves: early identification and effective safeguarding intervention.
- Benefit for users: children get help sooner; everyone feels listened to and protected.

Education: confident learners and informed adults

- We teach online safety to build knowledge, skills, attitudes and resilience—so learners can enjoy the benefits of technology while managing risks.

Planned learning for learners

- Online safety education is progressive, inclusive and revisited regularly. We use learner voice to shape what we teach and to keep it relevant.
- What this improves: safer choices, healthier online behaviour, and confident help-seeking.
- Benefit for users: learners become better prepared for real-life online challenges.

Staff training that supports safeguarding practice

- All staff receive induction and ongoing updates so they can spot concerns, respond appropriately, and model safe practice. Key roles receive enhanced training to lead and make informed decisions.
- What this improves: confidence and consistency across the workforce.
- Benefit for users: concerns are handled calmly, correctly and promptly.

Governors trained to provide challenge and support

- Governors/trustees understand their duties and can ask the right questions about policy, training, curriculum, filtering/monitoring, and cyber security.
- What this improves: accountability and sustained improvement.
- Benefit for users: online safety stays a priority over time, not just after incidents.

Strong partnerships with families and agencies

- We communicate practical guidance to families and work with relevant partners. We also share effective practice beyond our school where it supports safer communities.
- What this improves: joined-up messages and earlier support.
- Benefit for users: children experience consistent expectations across school and home.

Technology: protection that enables learning

- We use proportionate technical controls to reduce exposure to harm while supporting teaching and learning.

Effective filtering

- Filtering reduces the risk of access to harmful and illegal content and is reviewed to ensure it stays fit for purpose.
- Benefit for users: safer browsing and research.

Safeguarding-led monitoring

- Monitoring helps identify concerns early and supports timely intervention, handled with appropriate governance and data protection.
- Benefit for users: timely intervention when risk is emerging.

Secure systems and cyber resilience

- We protect networks, devices and accounts, and we prepare for threats like phishing and ransomware—so learning is not disrupted and users are protected.
- Benefit for users: safer services, fewer incidents, faster recovery.

Data protection that builds trust

- We handle personal and sensitive information carefully and lawfully, with clear processes and accountability.
- Benefit for users: privacy is respected and risks from misuse are reduced.

Safe day-to-day practice

- We manage devices consistently (including expectations around personal devices where relevant), apply safeguarding and consent to digital content, and communicate responsibly through our public channels.
- Benefit for users: fewer avoidable mistakes and a safer, more responsible digital culture.

Impact: proving what works and improving what doesn't

- We regularly review how well our policies and practice are working, what the evidence tells us, and what we will improve next. This keeps our approach current, targeted and effective.

How to raise a concern or get help

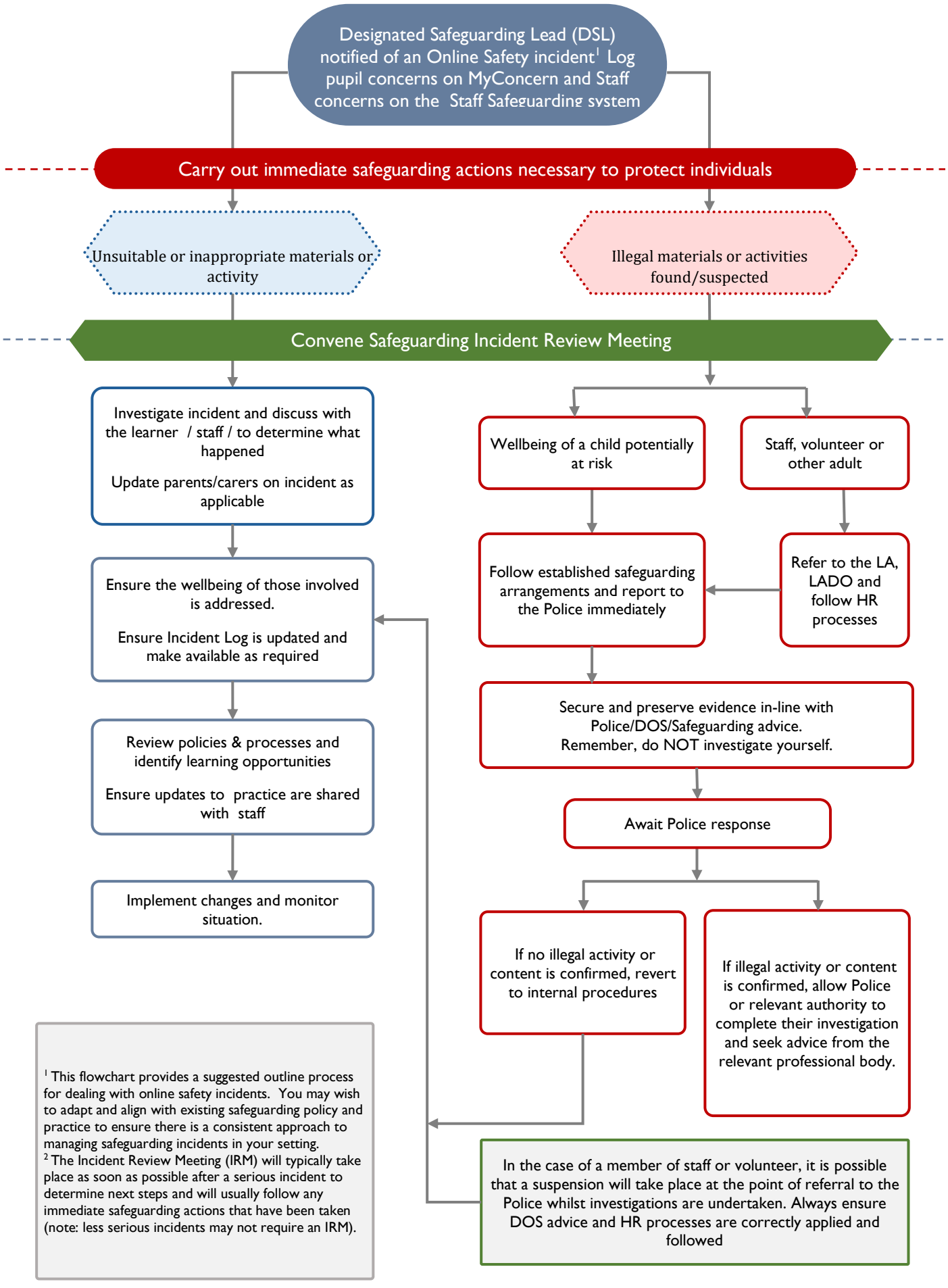
If something online worries you, we want to know.

- Learners: talk to a trusted adult, your tutor/class teacher, or the safeguarding team.
- Parents/carers: contact Julia Bray
- Staff: follow safeguarding procedures and record concerns promptly.

Our commitment

We will keep strengthening leadership, education, technology and impact review so that technology at Northiam Primary School is used safely, respectfully and positively—and so our community can be confident that online safeguarding is robust, consistent, and always improving.

Appendix A8 Responding to incidents of misuse – flow chart



Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.
A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about the Cyber Choices programme. Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

The Data (Use and Access) Act 2025 (DUAA)

Updates, rather than replaces, existing UK data protection law, including UK GDPR and the Data Protection Act 2018. For schools, the fundamental requirements to handle personal data lawfully, fairly, transparently and securely remain, but the Act introduces and clarifies provisions relating to areas such as lawful processing, automated decision-making, data sharing and the handling of data protection complaints. Schools should review their data protection policies, privacy information and procedures to ensure they reflect the changes, paying particular attention to how pupil, staff and parent/carer data is collected, accessed, shared and used, and to the use of emerging technologies and online services that process personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for

your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices for DfE guidance)

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online
https://www.gov.uk/guidance/what-academies-free-schools-and-colleges-should-publish-online

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Online Safety Act 2023

The Online Safety Act 2023 is a new set of laws that protects children and adults online. It puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms. The Act will give providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

Ofcom is the independent regulator of Online Safety. It will set out steps providers can take to fulfil their safety duties in codes of practice. It has a broad range of powers to assess and enforce providers' compliance with the framework.

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools / Resources for Schools / other organisations
Whisper Anonymous Reporting Tool - https://swgfl.org.uk/products/whisper/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
SWGfL Test filtering - http://testfiltering.com/
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations
Childline – Report / Remove
SWGfL- Assisted Monitoring
SWGfL – Resources for Education
DfE Using AI in education settings: support materials

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum
SWGfL Evolve - https://projectevolve.co.uk
SWGfL - ProjectEvolveEdu
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools
Teach Today – www.teachtoday.eu/

Data Protection
DfE – Data Protection in schools toolkit
ICO Guides for Organisations
ICO Guidance on taking photos in schools

Professional Standards/Staff Training
DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
UK Safer Internet Centre Professionals Online Safety Helpline
SWGfL – Online Safety Training

Infrastructure/Technical Support/Cyber-security
DfE – Technical Standards for Schools and Colleges
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
SWGfL- Assisted Monitoring
Secure Schools – Cyber Security

Working with parents and carers
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent
Prevent Duty Guidance
Childnet – Trust Me

Research
Ofcom – Childrens Media Habits
Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework