Pendle
Education Trust

Casterton Primary Academy

Online Safety Policy

Author of Policy	Raz Taj, DSL
Policy Approved by	Local Academy Council
Date	Nov 2025
Review Date	Nov 2026

Pendle Education Trust
Nelson and Colne College, Scotland Road, Nelson, BB9 7YT
Tel 01282 440 249 Email contact@pendleeducationtrust.co.uk
Company Registration Number: 08263591
Place of Registration: England and Wales

1 Policy and leadership

1.1 Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Casterton Primary Academy to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Casterton Primary Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

1.2 Policy development, monitoring and review

This Online Safety Policy has been developed by the Designated Safeguarding Lead (DSL) in consultation with the Principal, Safeguarding Governor and Pendle Education Trust (PET) DSL Cluster and Online Safety Group.

1.3 Schedule for development, monitoring and review

This Online Safety Policy was approved by the local academy council on:	Nov 2025
The implementation of this Online Safety Policy will be monitored by:	Raz Taj (DSL) and PET DSL Cluster and Online Safety Group
Monitoring will take place at regular intervals:	Termly in Online Safety Group meetings with a full review annually in the Spring term.
The Online Safety Group will receive a verbal update on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	Termly in Online Safety Group meetings.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Nov 2026

1.4 Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents from CPOMS
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Surveys/questionnaires of children, parents/carers, staff.

1.5 Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

1.5.1 Principal and Senior Leadership Team (SLT)

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the DSL as defined in Keeping Children Safe in Education (KCSiE).
- The Principal and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1].
- The Principal is responsible for ensuring that the Designated Safeguarding Lead, PET IT technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Principal and DSL will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Principals will receive regular monitoring reports from the Designated Safeguarding Lead.
- The Principal will work with the Safeguarding Governor, DSL and PET IT Team in all aspects of filtering and monitoring.

[1] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority / PET / HR / other relevant body disciplinary procedures.

1.5.2 Governors – Local Academy Council (LAC)

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".
This review will be carried out alongside the PET DSL Cluster and Online Safety Group whose members will receive regular information about online safety incidents and monitoring reports. A member of the local academy council will take on the role of Safeguarding governor, which includes responsibility for Online Safety to:

- have regular meetings with the Designated Safeguarding Lead
- regularly receive (collated and anonymised) reports of online safety incidents
- check that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- ensure that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by the DSL, and the IT service provider / PET IT Team and involve the responsible governor) – in accordance with the DfE Filtering and Monitoring Standards
- report to the local academy council
- receive (at least) basic cyber-security training to enable the governing body to check that the school meets the DfE Cyber-Security Standards

The local academy council will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

1.5.3 Designated Safety Lead (DSL)

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet regularly with the Online Safety Group and safeguarding governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant local academy council meetings/groups.
- Report regularly to Principal and SLT.
- Be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and PET IT Team on matters of safety and safeguarding and welfare (including online and digital safety).

- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- Have the leading role in establishing and reviewing the school online safety policies/documents.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- Liaise with curriculum leaders and teachers to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/children.
- Liaise with IT technical staff, pastoral staff and support staff (as relevant).
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing with regard to the areas defined in KCSiE:
    - content
    - contact
    - conduct
    - commerce
- Lead the Online Safety Group.

1.5.4 Curriculum Leader

The Computing Curriculum Leader will work with the DSL to develop a planned and coordinated online safety education programme based on the Education for a Connected World Framework and ProjectEVOLVE resources.

This will be provided through:

- Computing curriculum, including Online Safety
- PSHE curriculum
- Assemblies and additional pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day.

1.5.5 Teaching and support staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- They have read, understood, agreed to follow and signed the PET ICT Staff Acceptable Use Agreement (AUA).

- They follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- All digital communications with children, parents and carers and stakeholders should be on a professional level and only carried out using official school systems and devices (where staff use AI for this purpose, e.g. in the writing of reports, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements).
- They immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure children understand and follow the relevant parts of the Online Safety Policy and SHINE charter (by way of a pupil code of conduct / AUA), have an age/developmentally appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned children are guided to sites checked as suitable for their use and that they are aware of the processes in place for dealing with any unsuitable material that is found in internet searches.
- Where remote learning takes place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies, risk assessments conducted by the school.
- There is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media (both for professional and personal purposes).
- They adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity.
- They have a general understanding of how the children in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies.
- They are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services and prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

1.5.6 IT Provider / PET IT Team

The PET IT Team and IT Provider is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body.
- There is clear, safe, and managed control of user access to networks and devices.
- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the DSL or Principal for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring systems are implemented and regularly updated as agreed in school policies.

1.5.7 Children

- Are responsible for using the school digital technology systems in accordance with the Children's SHINE Charter.
- Should understand at an age/developmentally appropriate level the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

1.5.8 Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website.
- Providing them with a copy of the SHINE charters when their child starts school and by asking parents/carers to acknowledge these by signing the document as means of agreeing to the principles therein.
- Publish information about appropriate use of social media relating to posts concerning the school.
- Seeking their consent concerning digital images, cloud services etc. when their child starts school.
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- Reinforcing the online safety messages provided to children at home and upholding the principles of online safety in the SHINE charters.
- Ensuring their children do not bring personal devices, including mobile phones and smart watches to school under any circumstances.

1.5.9 Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

1.6 Online Safety Group

The PET DSL Cluster and Online Safety Group is made up of:

- Senior Leaders / DSL of all the PET schools
- Online Safety Leads of all the PET schools (where this leader is not the DSL)
- School staff, including Teaching Assistants and Technical Staff
- PET IT Technical staff
- PET Board Members

Members of the Online Safety Group will assist the DSL with:

- The production/review/monitoring of the school Online Safety Policy and related documents.
- The production/review/monitoring of the PET Technical Security Policy and requests for filtering changes.
- Mapping and reviewing the school's online safety curriculum – ensuring relevance, breadth, progression and coverage.
- Reviewing network/filtering/monitoring/incident logs.

- Encouraging the contribution of children to staff awareness, emerging trends and the school online safety provision.
- Consulting stakeholders – including staff/parents/carers about the online safety provision.

1.7 Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

- There is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Children will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence.
- There is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes.
- Policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.
- In the unlikely event that Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

2 Policy

2.1 Online Safety Policy

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- Allocates responsibilities for the delivery of the policy.
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.
- Describes how the school will help prepare children to be safe and responsible users of online technologies.

- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- Is supplemented by a series of related acceptable use agreements and other procedures.
- Is made available to staff at induction and in the staff handbook.
- Is published on the school website.

2.2 Acceptable use

The school has defined what it regards as acceptable/unacceptable use, and this is shown in the tables below.

The PET Staff ICT Acceptable Use Agreement (AUA) is shared with all staff at induction and at the start of every academic year thereafter. Staff members must confirm that they have read, understood and will follow the AUA at induction and then annually at the start of every academic year.

The PET Visitor AUA (which is signed by any visitor using school devices, as well as volunteers, students (including work experience placements), supply staff, agency staff, contractors, community users and parents) is shared with visitors at the point at which they require access to school systems/devices or induction in the case of supply staff / work experience placements etc. that are working in school over a longer period.

The AUA for children and parents/carers is part of the SHINE charters that are shared with children and parents/carers when a child starts school and by asking parents/carers to acknowledge these by signing the document as means of agreeing to the principles therein. The SHINE charters are on the school website, on display around the school building and are shared periodically in the school newsletter.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences – harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering *Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990):	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent children becoming involved in cyber-crime and harness their activity in positive ways – further information here.					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

When undertaken for non-educational purposes and using school devices / systems (unless otherwise stated)	Staff and other adults				Children	
	Not allowed	Allowed	Allowed at certain times/places	Allowed for selected staff	Not allowed	Allowed
Online gaming	X				X	
Online shopping / commerce			X		X	
File sharing	X				X	
Social media (personal use)	X				X	
Social media (professional use – PET /PPA accounts)		X			X	
Messaging / chat	X				X	
Entertainment streaming services (when used legally)			X		X	
Use of video broadcasting, e.g. YouTube, TikTok	X				X	
Personal mobile phones brought in to school		X			X	
Use of personal mobile phones in school			X		X	
Taking photos / images on personal mobile phones			X		X	
Use of other perianal digital devices, including tablets, gaming devices and smart watches			X		X	
Use of personal email accounts on school devices and/or school network/WiFi			X		X	
Use of school email for personal communication	X				X	
Use of AI services that have not been approved by school.	X				X	

When using communication technologies, the school considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- Any digital communication between staff and children or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media accounts must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
- Users should immediately report to the DSL the receipt of any communication that may be linked to school that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media accounts – see also: PET Social Media policy.

2.3 Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The DSL and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism /extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances

        - Cyber or hacking offences under the Computer Misuse Act
        - Copyright theft or piracy
- Any concern about staff misuse will be reported to the Principal, unless the concern involves the Principal, in which case the complaint is referred to the Chair of Governors and the CEO of Pendle Education Trust.
- Where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss.

Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more members of SLT should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by children and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed by the members of SLT conducting the check.
- Once this has been completed and fully investigated the members of SLT will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by Pendle Education Trust
    - Police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer and/or wellbeing support for those reporting or affected by an online safety incident.
- Incidents should be logged. Incidents involving children will be logged, including actions taken on CPOMS. Incident involving adults, including actions taken on StaffSafe.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.

- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- Learning from the incident (or pattern of incidents) will be provided anonymously and redacted as required to:
    - The DSL Cluster and Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with.
    - Staff, through Safeguarding Briefs and/or staff meetings
    - Children through assemblies and lessons
    - Parents/carers, through newsletters, school social media, website
    - Local academy council and PET Board through regular safeguarding updates and reporting.
    - Local authority/external agencies, as relevant

The school will make the flowchart on the following page available to staff to support the decision-making process for dealing with online safety incidents.

2.3.1 School actions

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.

2.4 The Prevent Duty

The Prevent duty, outlined in the Counter-Terrorism and Security Act 2015, requires schools to have "due regard to the need to prevent people from being drawn into terrorism." This includes addressing the risk of online radicalisation. Casterton Primary Academy recognises that the internet and social media can be used to spread extremist ideologies.

2.4.1 Filtering and Monitoring

The school has robust filtering systems to block access to extremist content, working alongside robust monitoring procedures to identify potentially concerning online activity.

2.4.2 Education and Awareness

Online safety education is integrated across the curriculum, including lessons at an age and developmentally appropriate level on:

- Identifying and reporting extremist content.
- Understanding the dangers of online grooming and manipulation.
- Promoting British values.

2.4.3 Staff Training

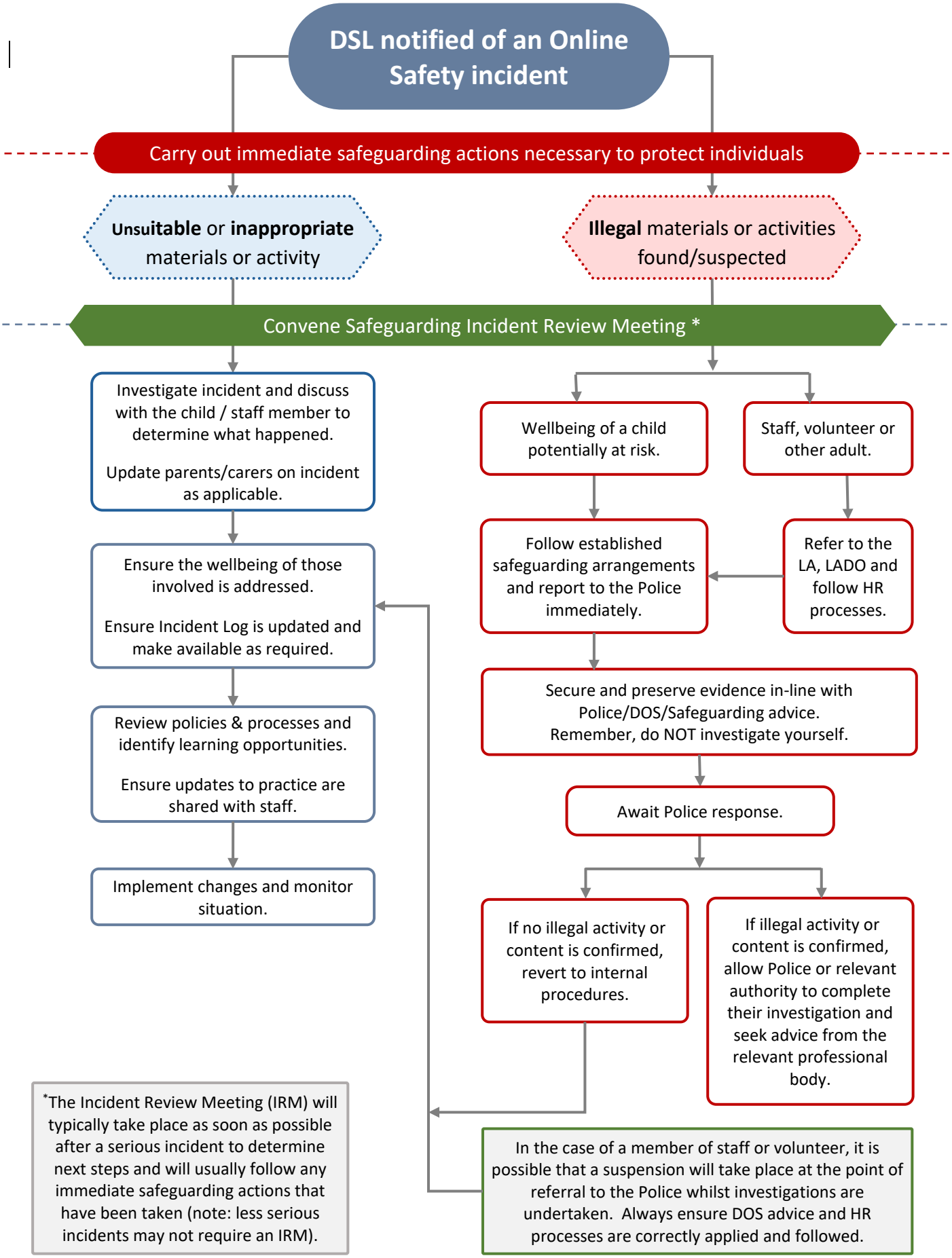
Staff complete Prevent Duty training on induction and biennially thereafter, alongside regular updates about recognising the signs of potential radicalisation and to understand their responsibilities under the Prevent duty.

2.4.4 Safeguarding Procedures

Safeguarding procedures are in place to address concerns about potential radicalisation. This includes clear reporting mechanisms and collaboration with relevant agencies. *See also: Prevent Duty Risk Assessment and Procedure.*

2.4.5 Parental Engagement

The school communicate with parents about online safety and the Prevent duty through the school newsletter, website and online safety information events, including at parent evenings. The school provides resources and guidance to help parents/carers keep their children safe online.


DSL notified of an Online Safety incident
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 child / staff member 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.
*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).
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.

2.4.6 Responding to incidents involving children's actions

Incidents	Refer to class teacher	Refer to Key Stage Leader	Refer to DSL or Principal	Refer to Police / CSC	Refer to PET IT Team for support / action	Inform parents/carers	Remove device / internet access rights	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).			X	X	X	X	X	X
Attempting to access or accessing the school network, using another user's account (staff or child) or allowing others to access school network by sharing username and passwords		X	X			X	X	X
Corrupting or destroying the data of other users.		X				X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature			X			X		X
Unauthorised downloading or uploading of files or use of file sharing.		X			X			X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.			X		X	X		
Deliberately accessing or trying to access offensive or pornographic material.			X		X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X						
Unauthorised use of digital devices (including taking images)		X	X			X	X	X
Unauthorised use of online services		X						X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X			X	X	X
Continued infringements of the above, following previous warnings or sanctions.			X			X	X	X

2.4.7 Responding to incidents involving staff actions

Incidents	Refer to line manager	Refer to Principal	Refer to HR	Refer to Police and/or LADO	Refer to PET IT Team for support / action	Issue a warning / management instruction	Further action, in line with disciplinary procedures
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X	X		X
Actions which breach data protection or network / cyber-security rules.		X	X		X	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X	X	X
Using proxy sites or other means to subvert the school's filtering system.		X	X		X	X	X
Unauthorised downloading or uploading of files or file sharing		X	X		X	X	X
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)		X	X		X	X	X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X	X		X	X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X	X	X
Using personal e-mail/social networking/messaging to carry out digital communications with children and parents/carers		X	X			X	X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X	X			X	X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X						
Actions which could compromise the staff member's professional standing	X						
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X				X	
Failing to report incidents whether caused by deliberate or accidental actions	X	X				X	
Continued infringements of the above, following previous warnings or sanctions.		X	X				X

3 The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (Gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently three key dimensions of AI use in schools: child support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

Casterton Primary Academy recognise that there are risks involved in the use of Gen AI services and that these services and therefore the risks are rapidly changing but that these risks can be mitigated through our existing policies and procedures, amending these as necessary to address the risks as they become apparent.

The school will educate staff and children about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and children will, as always, be at the forefront of our policy and practice.

3.1 AI Policy Statements

- Casterton Primary Academy acknowledges the potential benefits of the use of AI in an educational context – including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and children for a future in which AI technology will be an integral part. Staff are encouraged to use AI-based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- The school will comply with all relevant legislation and guidance, with reference to guidance contained in KCSiE and UK GDPR.
- The school will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. Supporting staff in identifying training and development needs to enable relevant opportunities.
- The school will seek to embed learning about AI as appropriate in our curriculum offer, including supporting children to understand how Gen AI works, its potential benefits, risks, and ethical and social impacts at an age and developmentally appropriate level. The school recognises the importance of equipping children with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the PET Staff ICT AUA, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information unless explicitly vetted for that purpose.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards with the PET IT Team before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes as these accounts are configured

to comply with organisational security and oversight requirements, reducing the risk of data breaches.

- The school will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the children, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the Principal and/or Data Protection Officer (DPO). Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, children and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school.
- AI tools may be used to assist teachers in the assessment of children's work, identification of areas for improvement and the provision of feedback. Teachers may also support children to gain feedback on their own work using AI.
- The school will maintain transparency in AI-Generated content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- The school will always prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- The school maintains recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action in accordance with the school's disciplinary procedures.

4 Online Safety Education

4.1 Online Safety across the curriculum

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against the Education for a Connected Work Framework and using Project Evolve resources is regularly taught in a variety of contexts.
- Lessons are sequenced, matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Child need and progress are addressed through effective planning and assessment, including the use of Project Evolve knowledge maps.
- Digital competency is planned and effectively threaded through links in other curriculum areas e.g. PSHE.
- Incorporating relevant national initiatives and opportunities e.g. Safer Internet Day.
- The curriculum is accessible to all children including those with Special Educational Needs and Disabilities (SEND) or those with English as an additional language (EAL).
- Children are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from AI services).
- Children are taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of AI services.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Children are helped to understand the need for online safety-related statements in the SHINE charter and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- Staff act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where children are allowed to freely search the internet, staff must be vigilant in supervising the children and monitoring the content of the websites / tools (including AI systems) the children visit.
- It is accepted that from time to time, for good educational reasons, children may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff must request the temporary removal of those sites from the filtered list for the period of study via an email to the DSL.

4.2 Staff

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety, cyber-security and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- Online safety training is an integral part of the school's CPD plan for all staff.
- All new staff will receive online safety training as part of their induction, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in a dedicated staff meeting.
- The DSL will provide advice/guidance/training to individuals as required.

4.3 Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- Attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Safeguarding Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and reviews.

4.4 Families

Many parents, carers and other family members have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes.
- Regular opportunities for engagement with parents/carers on online safety issues through awareness workshops, providing information at parents' evenings etc.
- The children – who are encouraged to pass on to parents/family members the online safety messages they have learned in lessons and by children leading sessions at parents' evenings.
- Letters, newsletters, social media and website information, including references to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers.
- High profile events / campaigns e.g. Safer Internet Day
- Sharing good practice with other schools via the PET DSL Cluster and Online Safety Group.

4.5 Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards families and relatives.
- Providing family learning courses in use of digital technologies and online safety.
- Providing online safety information via the school website and social media for the wider community.
- Supporting community groups, e.g. early years settings, youth / sports / voluntary groups to enhance their online safety provision.

5 Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school ensures that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

See also: PET Technical Security Policy (including filtering and passwords).

5.1 Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and PET IT Team and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the PET IT Team will have technical responsibility. The filtering and monitoring provision is reviewed termly by the PET DSL Cluster and Online Safety Group, which includes the DSL and the PET IT Team.

- Checks on the filtering and monitoring system are carried out by the PET IT Team with the involvement of the Designated Safeguarding Lead in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced.

5.2 Filtering

- The DSL and safeguarding governor, are responsible for ensuring that the DfE technical standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined.
- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE filtering standards for schools and colleges and the guidance provided by the UK Safer Internet Centre: Appropriate filtering.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes. All requests for changes to filtering must be made in writing via email.
- Filtering logs are regularly reviewed and alert the DSL to breaches of the filtering policy, which are then acted upon.
- There are monthly checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices and the results recorded and analysed to inform and improve provision. The DSL conducts the checks and makes the safeguarding governor aware of the findings. Checks on filtering are carried out using SWGfL Test Filtering, with the results saved for a period of one-year.

- Devices that are provided by the school have school-based filtering applied irrespective of their location.
- The school provides enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/children, etc.)
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
- Where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice. Internet access on personal devices in school is only available via Guest Wi-Fi.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content.

5.3 Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance.

The school has monitoring systems in place, agreed by SLT and technical staff, to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the DSL, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Monitoring provision is reviewed termly by the PET DSL Cluster and Online Safety Group, which includes the DSL and the PET IT Team and in response to changes in technology and patterns of online safety incidents and behaviours. The results of the review will be recorded and reported in the meeting minutes.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- Monitoring enables alerts to be matched to users and devices.
- Where AI –supported monitoring is used, the purpose and scope of this is clearly communicated.

5.4 Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges.

- Responsibility for technical security resides with the DSL, who may delegate activities to identified roles.
- A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff and children) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security to the DSL or PET IT Team.
- Password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre.
- All school networks, devices and systems will be protected by secure passwords.
- There is a risk-based approach to the allocation of children's usernames and passwords.
- There are regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling are securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- PET IT Team is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the DSL and/or PET IT Team.
- Use of school devices out of school by children and by family members is regulated by an acceptable use agreement that a child and their parent/carer consents to when the device is allocated to them.
- Use of school devices out of school by staff members is regulated by the PET Staff ICT Acceptable Use Agreement that is signed upon induction and at the start of each academic year thereafter.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.

- Staff members are not permitted to install software on a school-owned device without the consent of the PET IT Team.
- Removable media is not permitted unless approved by the SLT and/or PET IT Team.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit. *See also: PET Data Protection Policy and related documents.*
- Mobile device security and management procedures are in place.
- Guest users are provided with appropriate access to school systems based on an identified risk profile.
- Systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- Two-factor authentication is used for sensitive data or access outside of a trusted network.
- Where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias.

5.5 Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices e.g. smart watch, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud-based services such as e-mail and data storage. All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme. The school acceptable use agreements for staff; and for children, parents/carers in the form of the SHINE Charters.

The school does not allow children to bring personal digital devices into school under any circumstances, this includes the wearing of smart watches. ***See also: Behaviour, Anti-Bullying, Searching, Screening and Confiscation Policy.***

The school allows:

	School Devices		Personal Devices		
	School owned for individual use	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes			
Internet only				Yes – using Guest Wifi	Yes – using Guest Wifi
No network access					

School owned/provided devices:

- All school devices provided for use by children are managed though the use of Mobile Device Management software.
- There is an asset log that clearly states whom a device has been allocated to.
- There is clear guidance on where, when and how use is allowed.
- Personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated via the AUA.
- The use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- Liability for damage is covered in the AUA
- Education is in place to support responsible use.

Personal devices (Adult users only, children's personal devices are not permitted in school under any circumstances):

- There is a clear policy covering the use of personal mobile devices on school premises for all adult users.
- Where personal devices are brought to school, but their use is not permitted (e.g. in classrooms), appropriate, safe and secure storage is available.
- Use of personal devices for school business is defined in the acceptable use policy. Personal devices commissioned onto the school network are segregated effectively from school-owned systems via Guest Wifi.
- The expectations for taking/storing/using images/video aligns with the school's acceptable use policy. The non-consensual taking/using of images of others is not permitted. Under no circumstances should images/videos of children be taken or stored on personal devices.
- The school cannot accept liability for loss/damage or malfunction of personal devices brought into school.
- There is clear advice and guidance at the point of entry for visitors to acknowledge school requirements that personal devices not be used on school premises without prior agreement of a member of SLT.

- Education about the safe, appropriate and responsible use of personal mobile devices is included in the induction process.

5.6 Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children through:

- Ensuring that personal information is not published.
- Education for children and training for staff being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions.
- Risk assessment, including legal risk.
- Guidance for children and parents/carers.

School staff should ensure that when using personal social media accounts:

- No reference should be made to children, parents/carers or school/PET staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school/PET, this could be via the use of an appropriate disclaimer in their profile/bio.
- Security settings are regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media.

For official school social media accounts there is:

- A process for approval by the Principal for new accounts.
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff (this may include members of PET staff).
- Clear guidance in terms of acceptable use for users of the accounts.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

5.6.1 Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to personal social media sites during school hours on personal devices in line with the PET Staff ICT Acceptable Use Agreement.

5.6.2 Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media, the school will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

See also: PET Social Media Policy

5.7 Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff will inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images.

- Staff/volunteers must be aware of those children whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for taking photos of children under any circumstances.
- 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/performances 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 children in the digital/video images. Parents/carers will be reminded of this at the start of the event/performance.
- Staff are allowed to take digital/video images of children using school devices to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when taking/sharing digital/video images that children are appropriately dressed/positioned.
- Digital/video images published on the website, or elsewhere that include children will be selected carefully and will comply with Online Safety Policy, Social Media Policy, Data Protection Policy and be with parental consent.
- Children's full names will not be used anywhere on a website or social media, particularly in association with photographs, unless specific parental consent is obtained for this purpose.
- A written consent form from parents or carers will be completed before photographs of children are published/shared in any form. Parental consent is not required for images taken solely for internal purposes.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the relevant data protection and retention policies.
- Children's work can only be published with the permission of the child and their parents/carers.

5.8 Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- School website
- School social media accounts
- Online newsletters

The school website is managed by Juniper Education (from September 2025). The school ensures that online safety policy has been followed in the use of online publishing e.g., use

of digital and video images, copyright, identification of children, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where children's work, images or videos are published, their identities are protected, and full names are not published.

5.9 Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- Adheres to the Pendle Education Trust Data Protection Policy.
- Implements the data protection principles and can demonstrate that it does so.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO).
- Has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- Has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- The information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this.
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- Provides staff, parents, volunteers and children (where appropriate) with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- Has procedures in place to deal with the individual rights of the data subject.

- Carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions or entering into a relationship with a new supplier.
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data.
- Reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach, as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- Provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.
- Ensures that where AI services are used, data privacy is prioritised.

When personal data is stored on any mobile device or removable media the:

- Data on removable media will be encrypted, and password protected.
- Device will be password protected.
- Device will be protected by up-to-date endpoint (anti-virus) software.
- Data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
- Only use encrypted data storage for personal data.
- Will not transfer any school personal data to personal devices.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption, a secure email account and secure password protected devices.

5.10 Cyber Security

Pendle Education Trust IT Team has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards.

The PET Trust IT Team, working with the school:

- Will conduct a cyber risk assessment annually and review each term.
- Has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security.
- Has an effective backup and restoration plan in place in the event of cyber-attacks.
- Ensures the school's governance and IT policies reflect the importance of good cyber security.
- Ensures staff and members of the LAC receive training on the common cyber security threats and incidents that schools experience.
- Ensures the education programmes include cyber awareness for children.
- Ensures the school has a business continuity and incident management plan in place.
- Ensures there are processes in place for the reporting of cyber incidents. All staff (and children at an age and developmentally appropriate level) have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

6 Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, children; parents/carers and is reported to relevant groups.

- There is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training.
- There are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and the LAC.
- Parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising.

- Online safety and the related policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
- The evidence of impact is shared with other schools and agencies to help ensure the development of a consistent and effective local online safety strategy.

7 See also / related policies, procedures and documents

- SHINE Charters
- Behaviour, Anti-Bullying, Searching, Screening and Confiscation Policy
- Child-on-Child Abuse Procedure
- Prevent Duty Risk Assessment and Procedure
- Curriculum Policy
- Remote Learning Plan
- Curriculum Policy
- Curriculum Maps
- Curriculum Progression documents for Computing and PSHE
- PET Social Media Policy
- PET Technical Security Policy (including filtering and passwords).
- PET Staff ICT Acceptable Use Agreement
- PET Visitor ICT Acceptable Use Agreement
- PET Staff Code of Conduct