Pendle
Education Trust

Casterton Primary Academy

Online Safety Policy

Author of Policy	Raz Taj, DSL
Policy Approved by	Local Academy Council
Date	Sept 2024
Review Date	Sept 2025

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

Introduction

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. The legislative framework under which this Online Safety Policy and guidance has been produced is outlined in the attached 'Legislation' appendix.

This policy applies to all members of the school community (including staff, pupils, 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, anti-bullying policies, child-on-child abuse and child protection and safeguarding policies and procedures and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place both in and out of school.

The Online Safety Policy is based on a template from South West Grid for Learning (SWGfL) and has been developed by the Penlde Education Trust (PET) Online Safety Group. The PET Online Safety Group represents Casterton Primary Academy, Castercliff Primary Academy, Pendle Primary Academy, Colne Primet Academy and West Craven High School. The group comprises of a range of stakeholders, including:

- Senior Leadership Team (SLT) members, Designated Safeguarding Leads (DSL) and Deputy Designated Safeguarding Leads (DDSL)
- Staff – including teachers and support staff
- Members of PET ITL, Network and Support Teams
- Members of the schools' Local Governing Committees, which include parents and carers and community members
- Representatives of PET Trust Board

Consultation with each individual school's community has taken place through a range of formal and informal meetings.

The implementation and impact of this Online Safety Policy will be monitored by the PET Online Safety Group, which meets once a term and provides minutes of its meetings to each school's Local Academy Council. This 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.

Online Safety Policy

This Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- allocates responsibilities for the implementation 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 pupils in the digital world.
- describes how the school will help prepare pupils 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 related acceptable use agreements and procedures.
- is make known to new staff at induction and existing staff via the school website.

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.

Principal and Senior Leadership Team

- 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 may be delegated to the Online Safety Leader.
- The Principal and (at least) another member of SLT 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, which may include referral to the LADO.

- The Principal / DSL are responsible for ensuring that the Online Safety Leader, 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 / 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 Principal / DSL will receive regular monitoring reports from the Online Safety Leader.

Local Academy Council

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Local Academy Council, whose members will receive regular information about online safety incidents and monitoring reports. The named Safeguarding Link Governor will through meetings with the DSL / Online Safety Leader and review of Online Safety Group minutes and Safeguarding audits / report also oversee Online Safety on behalf of the Local Academy Council.

The Local Academy Council will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Leader

The Online Safety Leader is the Designated Safeguarding Lead (DSL) and a member of SLT.

The Online Safety Leader will:

- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.

- Have a leading role in establishing and reviewing the school online safety policies / procedures / documents.

- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.

- Liaise with curriculum leaders 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.

- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- Provide (or identify sources of) training and advice for stakeholders, including parents and carers.
- Liaise with the PET ITL team.
- Meet at least termly with the Online Safety Group to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and feed this information back to the Safeguarding Link Governor.
- Attend relevant Local Academy Council meetings.
- Report regularly to the Principal / SLT.

Designated Safeguarding Lead (DSL)

Casterton Primary Academy has a DSL and a number of deputies. These statements refer to the responsibilities of all trained DSLs (including Deputies) in the school. The DSLs are trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data.
- access to illegal/inappropriate materials.
- inappropriate on-line contact with adults/strangers.
- potential or actual incidents of grooming.
- online bullying.

It is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

Curriculum Leader and Subject Leading Teachers (Computing and PSHE)

Curriculum leads will work with the Online Safety Leader to develop a planned and sequenced online safety education programme based on the Education for a Connected World Framework and Project EVOLVE toolkit. Online Safety sits in both the Computing and PSHE curriculum progression documents and is also covered through assemblies and relevant national initiatives and opportunities such as Safer Internet Day and Anti-Bullying Week.

Teaching and Support 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 procedures.
- They understand that online safety is a core part of safeguarding.
- They have read, understood, and electronically 'signed' the PET IT Acceptable Use Agreement (AUA).
- They report any suspected misuse, problem or concern to a DSL or Deputy via CPOMS (if appropriate) for investigation/action, in line with the school safeguarding procedures.
- All digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all relevant aspects of the curriculum and other activities.
- Ensure pupils understand and follow the Children's SHINE charter and #BESAFE rules (see appendices), have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations at an age appropriate level.
- 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.
- Where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource.
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred, radicalisation etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of personal social media.

PET Information Technology for Learning (ITL) Team

Those with technical responsibilities working for PET and the school are responsible for ensuring:

- 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 PET in the Acceptable Use of ITL systems and resources policy.
- 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 / Online Safety Leader 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 software/systems are implemented and are regularly updated and evaluated.

Pupils

Pupils are responsible for, at an age-appropriate level:

- Using the school digital technology systems in accordance with the #BESAFE rules and Children's SHINE charter.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Knowing what to do if they or someone they know feels vulnerable / unsafe when using online technology.
- Understanding 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.

Parents / carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

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

- Publishing the school Online Safety Policy on the school website.
- Providing them with a copy of the Children's SHINE charter.
- Sharing information and advice about appropriate use of social media, online gaming and other relevant online safety issues, campaigns and literature.
- Seeking their permissions concerning publishing digital images, cloud services, internet use etc. via a parental consent form completed when their child starts school.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website
- School owned/provided digital devices provided for home learning.

Visitors

Visitors (including supply teachers, agency staff, contractors, visitors, community users, volunteers and parents) who access school systems or programmes at any time, including as part of the wider school provision will be expected to sign a Visitor ICT AUA (included as an appendices) 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.

Online Safety Group

The PET Online Safety Group provides a consultative group that has wide representation from the Trust and school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

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

- The production, review and monitoring of the school online safety policy and procedures and related policies and procedures.
- The production, review and monitoring of requests for filtering changes.
- Mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression.
- Monitoring network/internet/filtering/incident logs.
- Consulting stakeholders – including parents/carers and pupils about the online safety provision.
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool.

Professional Standards

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

Acceptable Use

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

The Online Safety Policy and related Acceptable Use Agreements (AUA) define acceptable use for stakeholders. The AUAs will be communicated/re-enforced through:

- SHINE Charters
- Staff induction, code of conduct and handbook
- Posters/notices where technology is used, e.g. #BESAFE rules
- Communication with parents/carers, e.g. newsletter
- Built into curriculum sessions and assemblies
- School website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & 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					**X**
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,					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	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)					
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. (Informed by the school's filtering practices and/or AUAs)				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 or other safeguards employed by the school				X	
	Infringing copyright				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	

Consideration should be given for the following activities when undertaken for *non-educational* purposes in school:	Staff and other adults				Pupils			
	Not allowed	Allowed	Allowed at certain times/places*	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Online gaming			X		X			
Online shopping / commerce			X		X			
File sharing			X		X			
Social media			X		X			
Messaging / chat			X		X			
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			X		X			
Personal mobile phones may be brought to school		X						X
Use of personal mobile phones at school			X		X			
Taking photos on personal mobile phones/cameras	X				X			
Use of other personal devices, e.g. tablets, gaming devices			X		X			
Use of personal e-mail in school, or on school network/Wi-Fi			X		X			
Use of school e-mail for personal e-mails	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 pupils 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 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 their line manager, a member of SLT or the DSL, the receipt of any communication 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 must be followed by staff when posting information online via official school channels, e.g. school website and social media.

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 child protection and 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 Designated Safeguarding Lead, Online Safety Lead 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 (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, which may include calling the Police and/or a referral to Children's Social Care.

- 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.

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

- One or more senior members of staff 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 pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). The same device will be used 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, if required.

- Once this has been completed and fully checked the senior staff involved 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 Casterton Education Trust senior staff

    - 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. support for those reporting or affected by an online safety incident.

- Incidents should be logged via CPOMS inline with the school's Child Protection and Safeguarding procedures or via StaffSafe if the allegation/concern about the conduct of a member of staff.

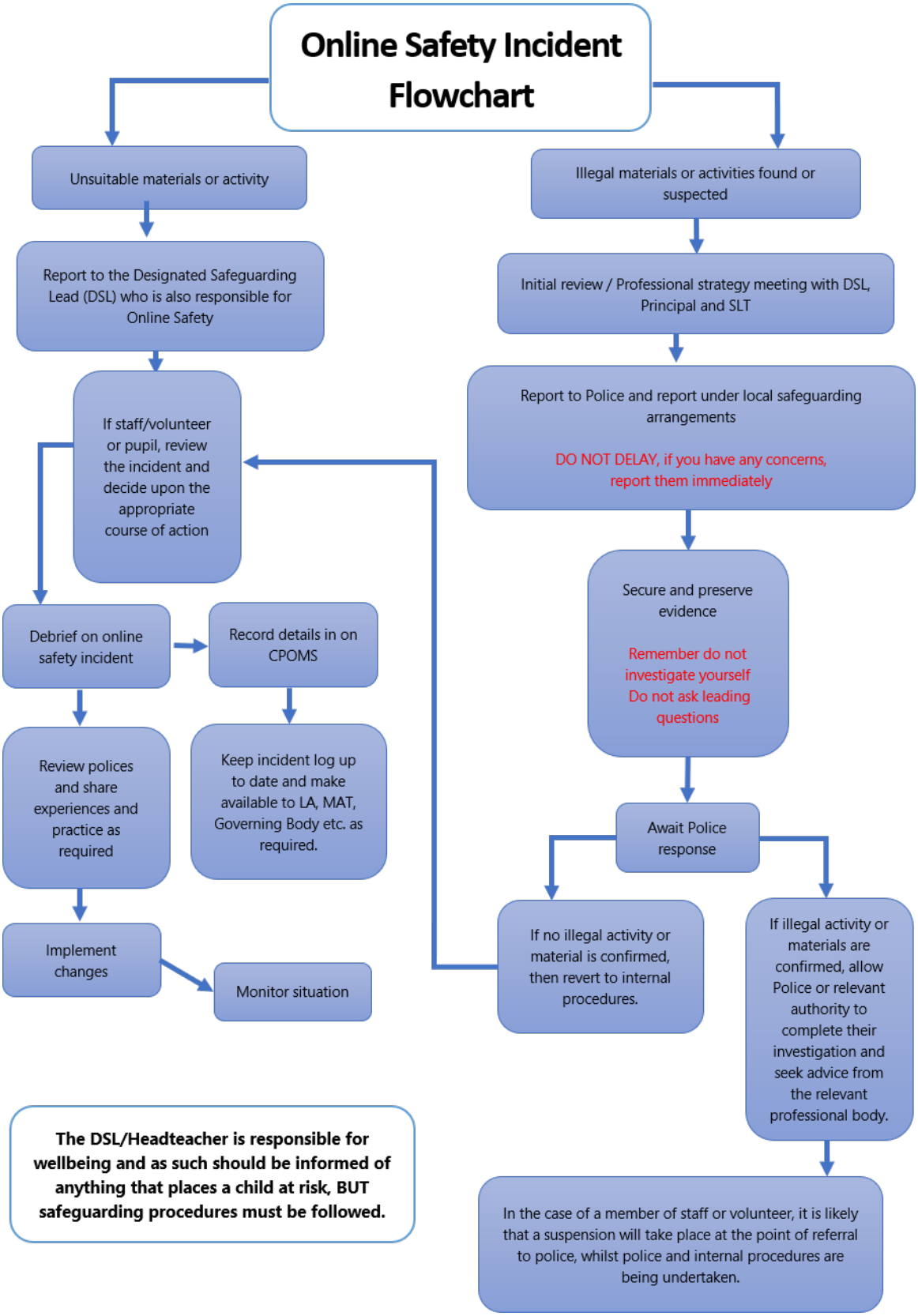
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.

- 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 (as relevant and anonymously) to:
    - The Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - Staff, through regular briefings
    - Pupils, through assemblies / lessons / interventions
    - Parents / carers, through newsletters, school social media, website
    - Governors, through regular safeguarding updates
    - Local authority / external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested, “working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”)

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

Online Safety Incident Flowchart



The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

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 as follows:

Responding to pupil actions: Incidents	Refer to class teacher	Refer to Key Stage Leader	Refer to DSL / Principal	Refer to Police / CSC	Refer to PET technical support for advice / action	Inform parents / carers	Remove device / network / 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 pupil) or allowing others to access school network by sharing username and passwords		X				X		X
Corrupting or destroying the data of other users.		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
Unauthorised downloading or uploading of files or use of file sharing.		X						

Responding to pupil actions: Incidents	Refer to class teacher	Refer to Key Stage Leader	Refer to DSL / Principal	Refer to Police / CSC	Refer to PET technical support for advice / action	Inform parents / carers	Remove device / network / internet access rights	Further sanction, in line with behaviour policy
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				X		X
Unauthorised use of digital devices (including taking images)		X				X		X
Unauthorised use of online services		X				X		X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X			X		X
Continued infringements of the above, following previous warnings or sanctions.			X		X	X	X	X

Responding to staff actions: Incidents	Refer to line manager / SLT	Refer to Principal / DSL	Refer to LADO	Refer to Police	Refer to IT and Network Support Team for action	Disciplinary action (e.g. warning, suspension)
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
Deliberate actions to breach data protection or network security rules.		X			X	X
Deliberately accessing or trying to access offensive or pornographic material		X			X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X
Unauthorised downloading or uploading of files or file sharing	X	X			X	
Breaching copyright or licensing regulations.		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
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X
Using personal e-mail / social networking / messaging to carry out digital communications with learners and parents / carers	X	X				X
Inappropriate personal use of digital technologies e.g. social media / personal e-mail	X	X				X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		X				X
Actions which could compromise the staff member's professional standing	X	X				
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X				X
Failing to report incidents whether caused by deliberate or accidental actions	X	X				
Continued infringements of the above, following previous warnings or sanctions.		X				X

Online Safety Curriculum / Education

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. Online safety forms a key part of Casterton Primary Academy's curriculum. The online safety curriculum should be broad, relevant and provide progression and will be provided in the following ways:

- A planned online safety curriculum for all year groups is matched against the Education for a Connected Work Framework is regularly taught in a variety of contexts, including the use of Project EVOLVE resources.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed learning targets leading to clear and evidenced outcomes.
- Pupil need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas in addition to PSHE and Computing.
- The Online Safety curriculum incorporates relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- The curriculum is accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- Pupils should be helped to understand the need for the #BESAFE rules and encouraged to adopt safe and responsible use both within and outside school.
- Staff should 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 pupils 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. This process is particularly important when asking children to engage in online research at home, where children may not be as closely monitored by an adult as they are in school.
- Where pupils are allowed to freely search the internet (KS2 only), staff should be vigilant in supervising the pupils and monitoring the content of the websites the pupils visit. Pupils use SWGfL Swiggle as a child friendly search engine, if asked to search freely under the close supervision of classroom staff.
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site and/or CEOP.

- It is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be made in writing via email to the Online Safety Leader, with clear reasons for the need.

- The planned online safety curriculum should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of pupils

The school acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of children. Their contribution is recognised through:

- Pupil surveys and interviews

- Appointment of academy ambassadors for each class

- Contributing to online safety education through school (e.g. presenting in assembly to peers), participating in events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff and volunteers

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 and data protection training will be made available to all staff. This will be regularly updated and reinforced.

- The training will be an integral part of the school's annual safeguarding and data protection training for all staff.

- Key online safety messages are included in the annual Safeguarding and Child Protection training provided to all members of school staff in Autumn term. Biennial Prevent training also covers elements of Online Safety. Dedicated online safety staff CPD takes place annually for teachers and TAs.

- An audit of the online safety training needs of all staff will be carried out periodically.

- All new staff will receive online safety input as part of their induction programme, 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 Online Safety Leader and Designated Safeguarding Lead 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 staff meetings / briefings / INSET days / twilights.

- The Online Safety Leader (or other nominated person, e.g. an alternative member of the Online Safety Group) will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training / awareness sessions. This may be offered in several ways such as:

- Online safety is included in annual governor safeguarding training.

- Attendance at training provided by the local authority/MAT or other relevant organisations, e.g. SWGfL, National Governors Association.

- Online accreditation / training opportunities (e.g. webinars).

- 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 the Online Safety / Safeguarding Link Governor.

Families

Many family members, including parents and carers 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 and family members with caring responsibilities may underestimate how often children and young people come across potentially harmful and inappropriate material online and may be unsure about how to respond.

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

- School website online safety pages https://www.castertonprimaryacademy.co.uk/online-safety/56.html, including links to relevant websites and advice.

- Regular communication to raise awareness and engagement on online safety issues and curriculum activities including: letters, newsletters, email and text messages.
- Parents' evening workshops / information sessions, including those that are pupil-led.
- Coffee Mornings
- Family learning workshops and drop-in events
- Promotion and participation in high profile events/campaigns e.g. Safer Internet Day
- Online safety messages targeted towards grandparents and other relatives as well as parents/carers.

Technology

The Pendle Education Trust ITL Team is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures outlined within this policy and detailed in the associated PET Technical Security Policy are implemented.

The Online Safety Leader is responsible for ensuring that all staff are made aware of policies and procedures in place and explain that everyone is responsible for online safety and data protection.

Technical Security

See: Pendle Education Trust Technical Security Policy (including filtering and passwords).

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, 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 devices in a school context is educational.

The Staff Acceptable Use Agreement (included as an appendices) and PET Staff Code of Conduct allows restricted use of personal mobile technologies on the premises for contracted school staff.

The Visitor Acceptable Use Agreement (included as an appendices) allows restricted use of personal mobile technologies on the premises. Visitors (including supply staff and volunteers) may be provided with the Wi-Fi password for use on personal devices in

circumstances agreed by the Principal or Online Safety Leader. This is will be upon the signing of the Visitor Acceptable Use Agreement.

Pupils are not permitted to carry or use personal digital devices in school; therefore, pupils do not have access to the academy's wireless network via personal digital devices. Any personal digital device (including, but not limited to, smartphones, tablets, laptops, smart watches) found in a pupil's possession, in school, will be confiscated and held securely in the school office until collected by a parent/carer. Such incidents will be reported on CPOMS and a meeting between a DSL or deputy and a parent/carer will take place to ensure safe use of the digital devices outside of school. This is in line with the school behaviour policy, where digital devices are listed as a prohibited item.

In order to ensure that learning continues, irrespective of enforced school closure or partial closure or self-isolation, the school has a limited number of laptops that can be provided to children for home learning purposes. These laptops are signed out and in from the school office by a parent/carer, who will have signed the Device loan agreement for pupils – parents (included as an appendices), which outlines acceptable/unacceptable use, data protection and damage/loss for the device whilst at home.

	School devices			**Personal devices**		
	School owned for individual use	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Allowed but not allowed to access on premises.	Yes	Yes
Full network access	Yes	Yes	Yes		No	No
Internet only					Yes	Yes – subject to signing Visitor AUA
Subject to school filtering / monitoring	Yes	Yes	Yes		Yes	Yes

Use on trips inc. residential visits	Yes	Yes	Yes	No	Yes – emergency use only if children are present	Yes – emergency use only if children are present
Taking / storing of pupil / staff images	Yes	Yes	Yes		No	No

Personal devices are brought into school entirely at the risk of the owner and the decision to bring the device in to school lies with the user as does the liability for any loss or damage resulting from the use of the device in school. The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).

Electronic Devices

- Pupils are not allowed to bring mobile phones or other personal electronic devices to school or use them in school. *See: Behaviour, Anti-Bullying and Exclusions policy.*

- Staff and visitors are allowed to bring personal electronic devices to school, although these must remain switched off and out of sight unless an Acceptable Use Agreement (see Online Safety policy) has been read and signed. Staff and visitors must adhere to strict restrictions of the use of personal electronic devices as described in the relevant Acceptable Use Agreement.

- Parents may use personal electronic devices in school in particular circumstances. All parents have signed a Parental Consent form (included as an appendices) outlining their responsibilities for appropriate use and sharing of images taken in school, e.g. a school events and performances. This policy refers to the searching for and of electronic devices and the deletion of data / files on those devices should there be concerns regarding inappropriate use of these devices.

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

- Authorised staff (including the Principal, Online Safety Leader and any trained DSL) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause

harm, disrupt teaching or break the school rules / terms of an agreed Acceptable Use Agreement.

- The authorised member of staff must have reasonable grounds for suspecting that an adult (staff member, visitor, contractor or parent) has used an electronic device in a way that contravenes the agreed terms of the Acceptable Use Agreements, or agreements made when signing in to school (for staff and visitors) or Parental Consent (for parents) before requesting to examine an electronic device in the possession of an adult.

- An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules / the agreed terms of an Acceptable Use Agreement). Accessing an electronic device found in the possession of a pupil should be done in the presence of a parent or carer where possible.

- As with all prohibited items, staff should first consider the appropriate safeguarding response if they find images, data or files on an electronic device that they reasonably suspect are likely to put a person at risk.

- Staff may examine any data or files on an electronic device they have confiscated as a result of a search if there is good reason to do so, e.g. if it:

    - poses a risk to staff or pupils;

    - is prohibited, or identified in the Behaviour policy for which a search can be made;

    - is evidence in relation to an offence.

- If the member of staff conducting the search suspects they may find an indecent image of a child (sometimes known as nude or semi-nude images), the member of staff should never intentionally view the image, and must never copy, print, share, store or save such images. When an incident might involve an indecent image of a child and/or video, the member of staff should confiscate the device, avoid looking at the device and refer the incident to the designated safeguarding lead (or deputy) as the most appropriate person to advise on the school's response. Handling such reports or concerns can be especially complicated and schools should follow the principles as set out in Keeping children safe in education. The UK Council for Internet Safety also provides the following guidance to support school staff and designated safeguarding leads: Sharing nudes and semi-nudes: advice for education settings working with children and young people.

- If a member of staff finds any image, data or file that they suspect might constitute a specified offence, then it must be reported and delivered to the police as soon as is reasonably practicable.

- In exceptional circumstances, members of staff may dispose of the image or data if there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files, the member of staff must have regard to the following guidance issued by the Secretary of State:

    - In determining whether there is a 'good reason' to examine the data or files, the member of staff should reasonably suspect that the data or file on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.

    - In determining whether there is a 'good reason' to erase any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

Care of confiscated devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices (particularly given the possible high value of some of these devices). Confiscated devices will be immediately taken by an adult to the office and placed in the school safe until they are collected by the owner or responsible adult (if the device was confiscated from a pupil).

Audit / Monitoring / Reporting / Review

Records are kept of incidents involving the searching for and of electronic devices and the deletion of data/files on CPOMS (where the incident involves a pupil) or Staff Safe (where the incident involves a member of staff).

Digital and video images

The school will inform and educate users about risks involving digital and video images and will implement policies to reduce the likelihood of the potential for harm.

The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.

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

Digital and video images of pupils must only be taken on school or PET-owned devices. The personal devices of staff, visitors or volunteers must never be used to take images of pupils.

Staff (including PET staff) must be aware of those pupils whose images must not be taken/published.

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 pupils in the digital/video images. This is agreed by all parents signing the Parental Consent Form for Photographs, Video, Cloud Storage and Internet use.

Staff are allowed to take digital/video images on school-owned 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 sharing digital/video images that pupils are appropriately dressed.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Photographs published on the school website, official social media or elsewhere that include pupils will be selected carefully.

Pupils' full names will not be used anywhere on a website or blog and never in association with photographs in which they are identifiable unless specific consent has been provided by a parent for this purpose.

Written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media, via the Parental Consent Form for Photographs, Video, Cloud Storage and Internet use.

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 school data protection policy.

Images will be securely stored on the OneDrive and retained only as long as all the children in the image remain in the school.

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils from social media through:

- ensuring that personal information is not published (unless, in specific circumstances, parental consent has been obtained to publish a child's name alongside their image, e.g. as a prize winner).

- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues for both staff and pupil users of social media.

- clear reporting guidance, including responsibilities, procedures and sanctions.

- risk assessment, including legal risk.

- guidance for pupils, parents/carers.

School staff should ensure that:

- no reference should be made in personal social media to pupils, parents/carers or school 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.

- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

- they act as positive role models in their use of social media.

- 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 as, *"views are my own"*. 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 mobile devices.

When official school social media accounts are established, there should be:

- a process for approval by senior leaders.
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- a code of behaviour 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.

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, a member of SLT 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.

Online publishing

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

- Public-facing websites, https://www.castertonprimaryacademy.co.uk/
- Social media: Facebook (Casterton Primary Academy) and Instagram *@castertonprimaryacademy*
- Online newsletters / letters published via the school website
- Texts messages
- Newspaper articles
- Print newsletters / letters / leaflets / posters and banners

The school website is managed/hosted by Content 4. 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 pupils, publication of school calendars and personal information, ensuring that there is least risk to members of the school community, through such publications.

Where pupil work, images or videos are published, their identities are protected, and full names are not published. Names are not published alongside pupil images unless additional parent consent has been obtained in specific circumstances, e.g. a prize presentation.

Data Protection

See: Pendle Education Trust GDPR Policy

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

- data 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 and that the computer/device is locked when leaving the room/workspace.
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes and review

The impact of this Online Safety policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; 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 Governors
- online safety (and 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, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendices

This policy should be read in conjunction with the following policies / procedures:

- Child Protection and Safeguarding Policy
- PET Technical Security Policy (including filtering and passwords)
- Social Media Policy
- PET GDPR Policy
- Behaviour, Anti-Bullying and Exclusions Policy
- Child-on-child Abuse Procedure
- DFE Keeping Children Safe in Education

Legislation

The legislative framework under which this online safety policy template and guidance has been produced is outlined below. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

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.

The National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". 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.

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.

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.

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.

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 2 years.

DfE "Keeping Children Safe in Education"

Guidance on Filtering and Monitoring

"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that 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 appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

Casterton Primary Academy

To #BESAFE when using digital devices and the Internet we will...

Casterton Primary Academy

Be polite and friendly when using online tools.

Explore the Internet safely, when an adult is with us.

Secret.

Never give out personal information and passwords.

Ask an adult if we need help using the Internet.

Freeze! Only click on buttons, icons and links when we know what they do.

Enjoy using the Internet but tell an adult straight away if we find something that upsets us.

#BESAFE (KS1)

Casterton Primary Academy

To #BESAFE when using digital devices and the Internet we will...

Casterton Primary Academy

Be polite and friendly when communicating using online tools and digital devices.

Explore the Internet safely, with the permission of an adult and when an adult is present.

Secret.

Never give out our own or others' personal information and passwords; be careful with the information that we share online.

Approved.

Only use Apps, programs and digital content that has been approved by an adult.

Freeze!

Immediately minimise any page containing content we are uncomfortable with and tell an adult.

Enjoy using the Internet and digital devices and make sure that others can do the same.

#BESAFE (KS2)

Children's SHINE Charter

Staff Acceptable Use Agreement

Pendle Education Trust – Staff ICT Acceptable Use Agreement (AUA)

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies 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. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Agreement is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Pendle Education Trust and each Academy's 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 will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff to agree to be responsible users.

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that all pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

If you have any concerns or require clarification on the any the points below, please discuss these with the Online Safety Leader/DSL or Academy Principal.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will only communicate with pupils and parents / carers regarding school matters using official school systems. Any such communication will be professional in tone and manner.
4. 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 from my own.
5. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
6. I will not be involved with any online activities, either within or outside school that may compromise my professional responsibilities or bring the school, staff, pupils or community into disrepute. This includes derogatory/inflammatory comments made on social network sites, forums, blogs and chat rooms.
7. I will ensure that my personal social media profiles have the appropriate privacy settings and include an appropriate disclaimer.
8. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory or those that are inappropriate or that may cause harm or distress to others.
9. I will respect copyright and intellectual property rights.
10. I will not use the school system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes).

11. I will not install any hardware or software myself. Any new hardware or software installations will only be arranged with the prior permission of the Computing or Online Safety Leader/DSL and Executive Director for ITL, and will be installed by the ITL team. I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
12. I will ensure that personal data is kept secure at all times and is used appropriately in accordance with Data Protection legislation. Under no circumstances should personal data be stored on any USB memory stick / portable hard drive or any other removable media.
13. I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
14. I will report any known misuses of technology, including the unacceptable behaviours of others.
15. I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
16. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable and may result in disciplinary action.
17. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
18. I have a duty to protect passwords and personal network logins, and should log off the network or lock my account when leaving workstations unattended. 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 understand that I should not write down or store a password where it is possible that someone may steal it.
19. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
20. I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.
21. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
22. I will take responsibility for reading and upholding the standards laid out in the AUA. I will support and promote the online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
23. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
24. I will take due care of any portable ICT equipment given to me to use for school purposes, and accept that if items (e.g. laptops, tablets) are taken offsite, that they are not insured for loss or damage caused by theft or accident. I understand that I will remain solely responsible for their replacement should, as a result of my own neglect or deliberate act, items be lost or damaged offsite.
25. I understand that portable ICT equipment provided for school purposes must not be used by non-members of school staff for any reason.
26. I will undertake Prevent training provided by the school and understand that I have the duty to report any online activities that could be linked to terrorist activity or radicalisation.

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Confirmation that this document has been read, understood and agreed must be made via the online form provided.

Visitor Acceptable Use Agreement

Pendle Primary Academy – Visitor ICT Acceptable Use Agreement (AUA)

Supply Teachers, Agency Staff, Contractors, Visitors, Community Users, Volunteers and Parents Agreement

To be read and signed by any adult (including parents) working in the school for a short period of time.

This Acceptable Use Agreement is intended to ensure:

- that community users of Pendle Primary Academy's 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 risk in their use of these systems and devices.

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 Pendle Primary Academy:

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory or those that are inappropriate or that my cause harm or distress to others.

3. I will respect copyright and intellectual property rights.

4. I will not use any camera or recording equipment (including mobile phones) without the prior agreement of the Online Safety Leader or Academy Principal. I will ensure that when images of pupils and/or adults are taken, they are stored and used only for professional purposes in line with academy policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside Pendle Education Trust without the prior permission of Pendle Primary Academy AND the parent/carer (when the subject is a child), or person(s) in the image (when the subject is an adult).

5. I understand that to use Wi-Fi provided by the school, a Trust Certificate must be applied to my device and that network activities and online communications are monitored, including any personal and private communications made using school systems.

6. I will not install any hardware (including removable media, e.g. USB memory sticks and portable hard drives) or software without the prior permission of the Academy Principal or Online Safety Leader. I understand that the use of any removable media may be subject to a checking procedure, which will be carried out by a member of school staff.

7. I understand that these rules are designed for the safety of all users and that if they are not followed, sanctions may be applied (the academy has the right to remove access to school systems / devices and to search personal devices used in the school), disciplinary action taken (if appropriate) and the police and other external agencies informed (if necessary).

8. I understand that the use of personal mobile phones is <u>not permitted</u> in classrooms or any other room where children may be present, between 8:30am and 4pm. Mobile phones should be SWITCHED OFF during the school day.

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

Signature _____ Date _____

Full Name _____ (PRINT)

Position/Role/Company _____