



West Exmoor Federation Online Safety Policy

Contents

Development/Monitoring/Review of this Policy	2
Schedule for Development/Monitoring/Review	2
Scope of the Policy	3
Roles and Responsibilities	4
Education and Information Statements	8
Federation responsibilities responding to:	
Peer on Peer Abuse, Cyberbullying, Sexting, Sexual Harassment, including Upskirting	11
Prevent	12
Technical – Infrastructure/equipment, filtering & monitoring	12
Data Protection	15
Use of digital images and sound	13
Communications	17
Assessment of risk	19
Responding to incidents of misuse	20
Illegal Incidents Flowchart	22
Record of reviewing responding to incidents of misuse	23
Reporting Log	24
Policy Review Log	25

This policy sets out the ways in which West Exmoor Federation will:

- educate all members of West Exmoor Federation on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of Online Safety;
- work to empower West Exmoor Federation to use technology including the internet as an essential tool for life-long learning.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and Federation s in England to ensure learners are safe from harm:

This policy is written in line with the latest 'Keeping Children Safe in Education' (KCSIE) statutory RSHE guidance and other statutory documents. This policy is used in conjunction with other Federation policies and has been developed by the Data Protection Officer and Caen Federation

The Online Safety policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to Online Safety or incidents that have taken place.

The Online Safety policy was approved by Governing body on 18th July 2024

The next review is due in July 2025

Scope of policy

This policy applies to all members of West Exmoor Federation, including staff, pupils, volunteers, parents/carers, visitors and users.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off West Exmoor Federation sites and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of Federation, but are linked to membership of West Exmoor Federation. It also applies to both staff and pupil use of technology for remote/online learning as part of a blended approach and during any Federation closures (partial or full) e.g. during a national/local lockdown or due to severe weather.

The DfE guidance “Keeping Children Safe in Education” sets out specific responsibilities for governing bodies to ensure:

- children are taught about online safety
- appropriate filters and appropriate monitoring systems are in place
- online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach

West Exmoor Federation will manage Online Safety as described within this policy and associated behaviour and anti-bullying policies and will inform parents and carers of known incidents of inappropriate Online Safety behaviour that take place in and out of the Federation.

This Online Safety Policy should be read in conjunction with the following other linked Federation policies:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- GDPR Data Retention Policy
- Social Media Policy
- Working Remotely Protocols

Roles and responsibilities

The Headteacher and Governors oversee the safe use of technology when children and learners are in their care and act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of West Exmoor Federation . They have concern for the online reputation of West Exmoor Federation.

KCSIE 2023 states that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)". The Headteacher who is the Online Safety Lead will have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying).

The Data Protection Officer will work the Online Safety Lead and designated safeguarding/online safety governor to update as required relevant policies and procedures so that implementation and monitoring of the Online Safety Policy and AUPs (Acceptable User Policies) follows best practice.

Role	Responsibility
Governors	• Approve the Online Safety Policy • Monitor the effectiveness of the Online Safety Policy¹ • Delegate a governor to act as Online Safety link • Online Safety Governor works with the Online Safety Lead to carry out regular monitoring and report to Governors • Verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online • Report to relevant governors/groups
Head Teacher (DSL) and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their Online Safety roles including online risks of extremism and radicalisation • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive Online Safety curriculum in place • Ensure that there is a system in place for monitoring Online Safety • Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious Online Safety issues • Ensure that West Exmoor Federation infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review Online Safety with West Exmoor Federation's technical support and Data Protection Officer. • Work with others in West Exmoor Federation involved in online safety and the Data Protection Officer to ensure that the Working Remotely Protocols implemented by West Exmoor Federation meets safeguarding and online safety requirements
DSL/Online Safety Lead (Head Teacher)	• 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 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 governing body meetings/groups • Report regularly to headteacher/senior leadership team • 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 IT providers on matters of safety and safeguarding and welfare (including online and digital safety) Lead the Online Safety working group • Coordinate work with West Exmoor Federation 's Designated Safeguarding Lead(DSL) and PSHE and Computing lead • Be responsible for logging, managing and informing others of Online Safety incidents and how they have been resolved where this is appropriate • In conjunction with the DPO, Lead the establishment and review of Online Safety policies and documents • Work with the PSHE/RSHE and Computing Leads to embed and monitor a progressive Online Safety curriculum for pupils, as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum • Ensure all staff are aware of the procedures outlined in policies relating to Online Safety • Liaise with the Data Protection Policy to provide and/or broker training and advice for staff • Attend updates, subscribe to appropriate newsletters and liaise with the LA Online Safety staff, technical staff and the Data Protection Officer • Meet with Senior Leadership Team, Online Safety Governor and the Data Protection Officer when applicable to regularly discuss incidents and developments
Curriculum Leads	Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE . This will be provided through: • a discrete programme • PHSE and SRE programmes • A mapped cross-curricular programme • assemblies and pastoral programmes • through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
All Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand, sign and act in accordance with the AUP and Online Safety Policy • Report any suspected misuse or concerns (within or outside Federation) to the Head Teacher (Online Safety Lead & Designated Safeguarding Lead (DSL) or Deputy DSL and check this has been recorded and actioned • Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum • Ensure all digital communications with learners and parents /carers are on a professional level and only carried out using official Federation systems • Model the safe, positive and purposeful use of technology

	• Monitor the use of technology in lessons, extracurricular and extended Federation activities, including Online/Remote Learning. • In lessons where internet use is pre-planned, learners are 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 • Be mindful of the additional safeguarding considerations required if delivering Online/Remote Learning • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with Federation ethos and policies, including at the time of a Critical Incident
Computing lead	• Work with the Online Safety and PSHE/RSE Leads to embed and monitor a progressive Online Safety curriculum for pupils, as part of the RSE Curriculum and to reinforce and extend learning within the Computing Curriculum
Pupils	• Read, understand, sign and act in accordance with the Pupil AUP / agreed class appropriate use of technology agreement • Report concerns for themselves or others • Make informed and positive choices when using technology in Federation and outside Federation, considering the effect on themselves and others • Should know what to do if they or someone they know feels vulnerable when using online technology
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss appropriate, healthy, safe use of technology and Online Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the internet • Keep up to date with issues through newsletters and other opportunities • Inform teacher / Headteacher of any Online Safety concerns • Use formal channels to raise matters of concern about their child(ren)'s education • Maintain responsible standards when referring to West Exmoor Federation on social media • Reinforce the online safety messages provided to learners in Federation
IT Provider	The DfE Filtering and Monitoring Standards says: <i>“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”</i> <i>“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”</i> <i>“The IT service provider (School's Broadband) should have technical responsibility for:</i> ○ <i>maintaining filtering and monitoring systems</i> ○ <i>providing filtering and monitoring reports</i> ○ <i>completing actions following concerns or checks to systems”</i> <i>“School's Broadband should work with the senior leadership team and DSL to:</i> ○ <i>procure systems</i>

	○ <i>identify risk</i> ○ <i>carry out reviews</i> ○ <i>carry out checks”</i> “We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within West Exmoor Federation, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision.” School's Broadband is responsible for ensuring that: • they are aware of and follow West Exmoor Federation Online Safety Policy and Technical Security Policy to carry out their work effectively in line with Federation policy • West Exmoor Federation technical infrastructure is secure and is not open to misuse or malicious attack • West Exmoor Federation meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Federation s & 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 Jayne Peacock 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 (see appendix 'Technical Security Policy template' for good practice). • monitoring systems are implemented and regularly updated as agreed in Federation policies
Users	• Sign and follow the Guest/Staff AUP before being provided with access to Federation systems • Demonstrate appropriate standards of personal and professional conduct in line with the AUP

Education of pupils

'Children are taught about safeguarding, including online safety. Federation s should consider this as part of providing a broad and balanced curriculum.'

Keeping Children Safe

A progressive planned Online Safety education programme takes place in line with 'Teaching online safety in Federation s', as part of Computing/PSHE, for all children in all years, and is regularly revisited.

Within this:

- key Online Safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all teaching
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies. They are taught a set of SMART rules which pupils are expected to follow at home and in Federation to make sure they stay safe online.
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- in lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches
- pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils are provided with opportunities to influence the online safety curriculum
- pupils will write and sign an AUP for their class at the beginning of each Federation year, which will be shared with parents and carers
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying' and given opportunities to support each other

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in Federation . They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. West Exmoor Federation supports parents and carers to do this by:

- providing clear AUP guidance which they are asked to sign with their children
- providing regular newsletter items and appropriate support materials
- raising awareness through activities planned by pupils and staff
- via parents evenings
- providing and maintaining links to up to date information on West Exmoor Federation website

Good advice for parents and carers

- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.
- Parents need to be aware that the parental control software doesn't replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online "friends". Only talk to people they know. Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.
- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.

Education of wider Federation

West Exmoor Federation provides information about Online Safety to organisations using Federation facilities, the Nursery and members of the wider community.

Training of Staff and Governors

There is a planned programme of Online Safety training as part of the overarching safeguarding approach, in line with Keeping Children Safe 2023 for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- all staff knowing the Designated Safeguarding Lead and the Online Safety Lead and their responsibilities
- all new staff and governors receiving Online Safety and Information Security training as part of their induction programme
- providing information to supply and student teachers on West Exmoor Federation 's Online Safety procedures
- the Online Safety Lead receiving regular updates through attendance at training sessions, updates from the Data Protection officer and by reviewing regular Online Safety newsletters from the LA
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings
- the Online Safety Lead providing training within safeguarding training and as specific online safety updates and reviews
- the Online Safety Lead providing guidance as required to individuals and seeking LA support on issues

Peer on Peer Abuse

All members of staff are made aware that children can abuse other children (often referred to as peer on peer abuse). Children are encouraged to talk to members of staff if they feel they are the victim or perpetrator, or if they are aware of peer on peer abuse. This abuse may include:

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of West Exmoor Federation will not be tolerated. Full details are set out in West Exmoor Federation's behaviour policy. West Exmoor Federation will follow procedures in place to support anyone in West Exmoor Federation affected by cyberbullying.

- Pupils and staff are made aware of a range of ways of reporting concerns about online bullying.
- Pupils, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.
- All incidents of online bullying reported to West Exmoor Federation will be recorded and action taken by West Exmoor Federation.
- West Exmoor Federation will follow procedures to investigate incidents or allegations of online bullying.
- West Exmoor Federation will take steps where possible and appropriate, to identify the bully. This may include examining Federation system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with West Exmoor Federation to support the approach to online bullying and West Exmoor Federation's Online Safety ethos.
- Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in West Exmoor Federation's Behaviour Policy or AUP and may include:
 - the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
 - internet access being suspended at West Exmoor Federation for a period of time.
 - the parent and carers of pupils being informed
 - the police being contacted if a criminal offence is suspected

Sexting

West Exmoor Federation will follow [UKCIS advice](#) on how to respond to any incident of sexting. We will provide appropriate support for sexting incidents which take place in and out of Federation. Within the Federation, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL). An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from Devon Local Authority.

Sexual Harassment, including Upskirting

All staff are made aware that sexual harassment can occur between two children of any age and sex and can include online harassment. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence and can include:

- non-consensual sharing of sexual images and videos
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation; coercion and threats
- upskirting

All staff are made aware of what upskirting is, and that it is illegal. Any incident of sexual harassment will be taken seriously and reported to the Designated Safeguarding Lead (DSL). The Designated Safeguarding Lead (DSL) will record the incident(s) and the actions taken in line with [DfE Guidance](#) and advice from Devon Local Authority and/or the police as necessary.

Prevent

West Exmoor Federation works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

Technical Infrastructure

The person(s) responsible for West Exmoor Federation's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP.

West Exmoor Federation ensures, when working with our technical support provider that the following guidelines are adhered to:

- West Exmoor Federation ICT systems are managed in ways that ensure that West Exmoor Federation meets Online Safety technical requirements
- there are regular audits of the safety and security of Federation ICT systems.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations and other devices from accidental or malicious attempts which might threaten the security of West Exmoor Federation systems and data with regard to:
 - ensuring ongoing backups take place and, in case of an incident, West Exmoor Federation can restore data in line with our business continuity plan
 - the downloading of executable files by users
 - the extent of personal use that users (staff/pupils/ users) and their family members are allowed on laptops and other portable devices used out of Federation
 - the installing of programs on Federation devices unless permission is given by SWGFL or Computing/ICT coordinator

- the use of removable media (e.g. memory sticks) by users on Federation devices. (see West Exmoor Federation's Data Protection Policy for further detail)
- the installation of up to date anti-virus software
- access to West Exmoor Federation network and internet will be controlled with regard to:
 - users having clearly defined access rights to Federation ICT systems through group policies
 - users being provided with an appropriate username and password (considering accessibility of users with particular needs where supervision is put in place to monitor activity)
 - staff users being made aware that they are responsible for the security of their username and password which they are required to change regularly as stipulated; they must not allow other users to access the systems using their log on details
 - the 'master/administrator' passwords for all systems are available to the Headteacher and kept securely in an agreed place
 - users must immediately report any suspicion or evidence that there has been a breach of security
 - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto West Exmoor Federation system. Anyone allowed unsupervised access must sign the staff AUP and be made aware of this Online Safety Policy
- the internet feed will be controlled with regard to:
 - West Exmoor Federation's responsibility to ensure appropriate filters and appropriate monitoring systems are in place. Children are safeguarded from potentially harmful and inappropriate online material." Keeping Children Safe. Refer to <https://www.saferinternet.org.uk/advice-centre/teachers-and-Federation-staff/appropriate-filtering-and-monitoring>
 - Foundation Stage and Key Stage 1 pupils' access will be supervised with access to specific and approved online materials
 - Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities
 - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged using the Request Form for Unfiltering a Website
 - user based filtering used to provide differentiated access for staff and pupils
 - filtering issues being reported immediately
- the IT System of West Exmoor Federation will be monitored with regard to:
 - West Exmoor Federation IT technical support regularly monitoring and recording the activity of users on West Exmoor Federation IT systems

- Online Safety incidents being documented and reported immediately to the Head Teacher or Deputy Designated Safeguarding Lead D(DSL) who will arrange for these to be dealt with immediately in accordance with Federation policies

Data Protection

West Exmoor Federation 's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

West Exmoor Federation will:

- at all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- provide staff with secure equipment/services to store or transfer data eg remote access, Google Drive, , encryption and secure password protected devices
- remove data in line with West Exmoor Federation 's GDPR Data Retention Policy
- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead and that relevant staff understand the full requirements of Data Protection Act 2018
- complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

Use of digital images and sound

Photographs, video and sound recorded within Federation are used to support learning experiences across the curriculum, to share learning with parents and carers on our Federation 's learning platform and to provide information about West Exmoor Federation on the website. West Exmoor Federation will:

- build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound
- ensure verifiable permission from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on West Exmoor Federation website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use
- when using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images, record video and sound to support educational aims, following West Exmoor Federation policy regarding the sharing, distribution and publication of those. Federation equipment only is used. Personal equipment of staff is not allowed for this purpose

- make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or West Exmoor Federation into disrepute
- make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed
- ensure that pupils' full names will not be used anywhere on West Exmoor Federation website, Federation blogs or within Federation branded social media, particularly in association with photographs.
- Where exceptional individual achievement may warrant the naming of an individual (such as winning a national title representing West Exmoor Federation (and this information will be available publicly on other websites), then a pupil's full name may be justified, with additional consent from parents. (This could be via email and consent must be obtained each time this occurs)
- not publish pupils' work without the permission of their parents or carers
- only hold digital/video images on Federation approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with West Exmoor Federation's Data Retention Policy
- in accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at Federation events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to 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 or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of West Exmoor Federation
- make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people

Communication (including use of Mobile Devices and Social Media)

A wide range of communications technologies increases effective administration and has the potential to enhance learning. West Exmoor Federation will:

with respect to email and other online communication tools (e.g. Microsoft Teams, Google Meet)

- ensure that West Exmoor Federation uses secure business systems for communication
- ensure that personal information is not sent via unsecure systems
- ensure that governors use secure systems
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that communications will be monitored by West Exmoor Federation
- inform users what to do if they receive online communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- teach pupils about email and other communication tools alongside safe, healthy appropriate use of technology and online safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this required
- protect the identities of multiple recipients by using bcc in emails

with respect to Online/Remote Learning opportunities e.g. Zoom, Google Classroom, etc.

- develop a strategic approach to Blended Learning which enables online/remote learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by West Exmoor Federation
- when selecting online learning platforms, first consider data protection. Complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
- make sure that access to platforms will be password protected and run with approval from the Senior Leadership Team
- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content

- discuss the use of online/remote learning as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice being careful about subjects discussed online
Refer to DfE Cyberbullying Advice for headteachers https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_Federation_Staff_121114.pdf and Teaching Standards 2012 <https://www.gov.uk/government/publications/teachers-standards>
- register concerns (e.g. recording in Online Safety log) regarding pupils' inappropriate use (in or out of Federation) and raise with their parents and carers
- support staff to deal with the consequences of hurtful or defamatory posts about them online

with respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- control access to social media and social networking sites in the Federation
- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age-appropriate b) whether content can be shared by the site or others without additional consent being given
- make sure that staff official blogs or wikis will be password protected and run with approval from the Senior Leadership Team
- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content
- discuss with staff the personal use of email, online learning platforms, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice, being careful about subjects discussed online
- staff are advised that no reference should be made to pupils, parents/carers or Federation staff on their personal social networking accounts
- register concerns (e.g. recording in Online Safety log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of Federation) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
- support staff to deal with the consequences of hurtful or defamatory posts about them online
- inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the Head Teacher.

with respect to personal devices (including consideration of Keeping Children Safe)

- inform staff that personal devices should only be used at break and lunchtimes in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher (turned off at other times)
- ensure that staff understand that the AUP will apply to the use of their own portable / wearable device for Federation purposes
- inform staff and visitors that they are not allowed to use personal devices to take photographs or video in Federation for any purpose without the express permission of SLT
- check any use of a personal device for an education purpose (where permission has been given) only uses West Exmoor Federation 's internet connection on West Exmoor Federation site
- remind all that personal devices should be pin-code or fingerprint protected and not discoverable by third parties
- remind staff of the importance of updating device operating systems and software updates to maintain the device's security (most of the updates are critical security updates)
- advise staff not to use their personal mobile phone to contact pupils, parents and carers, unless in an emergency situation or permission has been given by the Head Teacher
- provide a mobile phone for activities that require them
- challenge staff and visitors when there is suspected misuse of mobile phones or devices
- when pupils are allowed personal devices in Federation , they are used within West Exmoor Federation 's behaviour policy / code of conduct, and pupils understand they can be asked to account for their use
- use the right to collect and examine any pupil device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on West Exmoor Federation internet connection

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances West Exmoor Federation will examine and adjust the Online Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material

West Exmoor Federation provides appropriate filtering and monitoring as stated in this policy. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Federation device.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents

West Exmoor Federation will follow the SWGFL flowchart (see Appendix) to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Where content being reviewed is suspected or known to include images of child abuse, the investigation will be referred to the Police immediately and no further access will be made by West Exmoor Federation to the material.

- All members of West Exmoor Federation will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)
- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded
- The Designated Safeguarding Lead (DSL) will be informed of any Online Safety incidents involving child protection concerns, which will then be escalated in accordance with Federation procedures
- West Exmoor Federation will manage Online Safety incidents in accordance with West Exmoor Federation Behaviour Policy where appropriate
- West Exmoor Federation will inform parents and carers of any incidents or concerns in accordance with Federation procedures
- After any investigations are completed, West Exmoor Federation will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then West Exmoor Federation will contact Devon Children Safeguarding Team and escalate the concern to the police
- If West Exmoor Federation is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Service or Local Authority Designated Officer (LADO).

If an incident or concern needs to be passed beyond West Exmoor Federation , then the concern will be escalated to the Education Safeguarding Service to communicate to other education institutions in Devon. Should serious Online Safety incidents take place, the following external persons and agencies should be informed:	Education Safeguarding Service Local Authority Designated Officer (LADO)
---	--

The police will be informed where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images

- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

Sanctions and Disciplinary proceedings

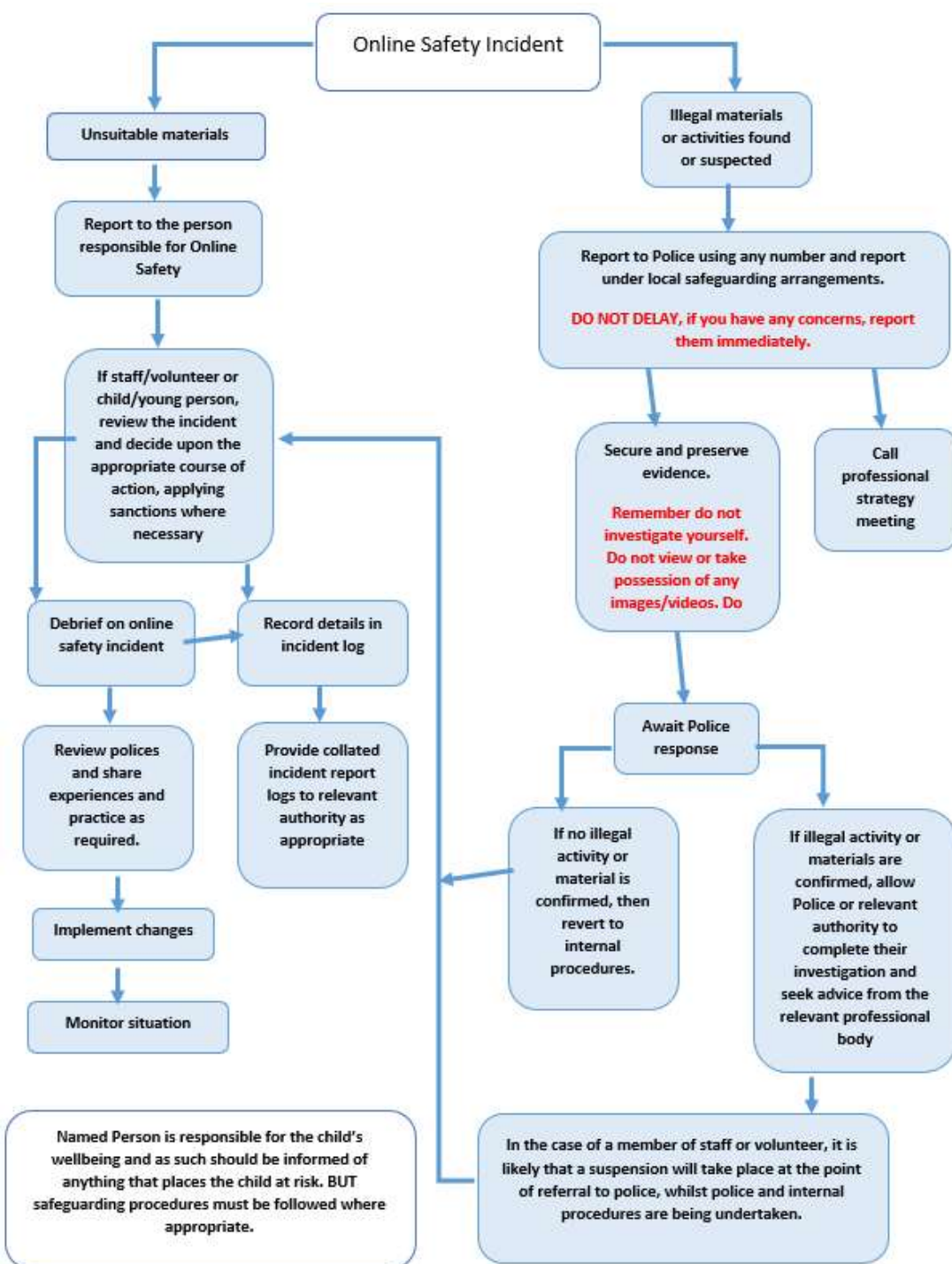
Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to (unless this is part of an investigation:

- child sexual abuse images
- grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity including radicalisation and terrorism
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of West Exmoor Federation or brings West Exmoor Federation into disrepute
- using Federation systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by West Exmoor Federation
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high-volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

Appendix

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Record of reviewing devices/internet sites (responding to incidents of misuse)

Date:
Reason for investigation:
.....
.....

Details of first reviewing person

Name:
Position:
Signature:

Details of second reviewing person

Name:
Position:
Signature:

Name and location of computer used for review (for web sites)

.....
.....

Web site(s) address/device	Reason for concern
Conclusion and Action proposed or taken	

Reporting Log						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Policy History

This Policy is maintained by the Data Protection Officer and will be reviewed on an annual basis. For help in interpreting this policy, please contact:

Gary Brock

Email: gary@gbrocksolutions.org

Policy Date	Summary of Change	Contact	Implementation Date
March 22	Added to the scope, removed training log, inserted additional good advice for parents, indicated when the use of full pupil names on website may be justified and added updates to the Acceptable Use policies to now include the requirement to keep personal devices operating system's updated to strengthen security.	DPO Gary Brock	24 March 2022
June 24	• Updated using latest ICO guidance using the SWGFL template • Updated legislation dates as required, • Included new/additional guidance in bold • Removed Technical Security, BYOD, AUPs and Social Media Policies which will be presented and updated as separate policies	DPO Gary Brock	2 nd June 2024

