Taywood Nursery School and Extended Services

Online Safety Policy

January 2024

Review date: January 2025

SWGfL
Safe, Secure, Online

Area One	Focus One	Focus Two	Focus Three	Focus Four
Management	Responsibilities	Policy	Practice	Safeguarding

Area Two	Focus One	Focus Two	Focus Three	Focus Four
People	Educating Children	Training Adults	Personal Data	Responding to Issues

Area Three	Focus One	Focus Two	Focus Three	Focus Four
Technology	Devices	Security	Digital Images	Social Media & Communication

Background / Rationale

The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work with children are bound.

Digital technologies are powerful tools that open up opportunities for everyone and have become integral to our lives. Children, staff and volunteers have a right to safer internet access at all times.

The use of these new technologies can put users at risk. Some of the dangers may include:

- Access to illegal, harmful or inappropriate images or other content
- Loss of privacy / control of personal information
- Grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers.
- Online-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Hacking, viruses and system security

- The potential for excessive use which may impact on children's social and emotional development and learning.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other policies (e.g. safeguarding / child protection policies).

As with all other risks, it is difficult to eliminate the risks completely. By providing good examples/role models and by raising awareness, it is possible to build the resilience of children, so that they have the confidence and skills to deal with these risks.

Settings should be able to demonstrate that they have provided the necessary safeguards to manage and reduce these risks.

Taywood Nursery School and Extended Services has a significant role to play in keeping children safe and that includes online. Whether we provide internet access or not, young children will usually have access to the internet at home and we need to ensure their safety and well-being wherever they are.

Much of the current legislation that requires Taywood Nursery School to effectively safeguard children and users now includes clear references to online harms e.g. Working Together to Safeguard Children includes online abuse and the influences of extremism leading to radicalisation.

When defining "abuse"

> *"Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults, or another child or children."*

Ofsted 'Inspecting Safeguarding' 2018 requires that

> *"Leaders oversee the safe use of technology when children and learners are in their care and take action immediately if they are concerned about bullying or children's well-being"*

Settings are held to account by this legislation and therefore it is important to reflect this within our setting's policy and practice.

The online safety policy that follows explains how we intend to do this.

Development / Monitoring / Review of this Policy

This online safety policy was developed by	*Mrs Jennifer Slater (Headteacher)*
These people / groups were involved / consulted in the development of the policy	• *Senior Leadership Team* • *Extended Services Co-ordinator- Claire Farr* • *Designated Safeguarding Lead (DSL)* • *Staff Online Safety Support- Talisha Bridge* • *Chair of Governors (Colin Woolford)* • *Parent Governor (Victoria Antcliffe)*
This online safety policy was approved by:	*The Governing Board*
On	*5th February 2024*
The implementation of this online safety policy will be monitored/reviewed by the:	• *Jennifer Slater* • *Designated Safeguarding Lead* • *Staff Online Safety Support- Talisha Bridge*
Monitoring/review will take place at regular intervals:	*Termly*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new development. The next anticipated review date will be:	*Annual review of this policy- January 2025*

Should serious online incidents take place, the following external persons / agencies should be informed:	Local Authority Designated Officer (LADO) Police

Scope of the Policy

This policy applies to all members of the setting (including staff/volunteers, children, parents/carers, visitors, community users) who have access to and are users of communications technologies (whether these belong to the setting or to the users themselves)

Management

Responsibilities

The following section outlines the roles and responsibilities for the online safety within the setting.

Role of the Headteacher

- The Headteacher (Jennifer Slater) has overall responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the setting, though the day to day responsibility for online safety may be delegated to others (*insert titles*).
- The Headteacher *(and Extended Services Co-ordinator)* 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 or volunteer. (see flow chart on dealing with online safety incidents – included in a later section)
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff/volunteers receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher will ensure that there is a system in place to allow for the monitoring of online safety in the group and that they receive regular monitoring reports.

Online Safety Lead

The Online Safety Lead: Jennifer Slater (Headteacher)

- ensures that staff/volunteers have an up to date awareness of the setting's online safety policy and practices and incident reporting procedures
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies/procedures

- offers advice and support for all users
- keeps up to date with developments in online safety
- understands and knows where to obtain additional support and where to report issues
- ensures provision of training and advice for staff/volunteers
- liaises with any national/local organisation (as relevant)
- receives reports of online safety incidents and keeps a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be found in the appendix)
- communicates with parents/carers
- monitors incident logs

The Online Safety Lead is aware of online safety issues and the potential for serious safeguarding issues and is capable of managing them effectively.

Staff/volunteers

Responsible for ensuring that:

- they have an up to date awareness of the setting's online safety policy and practices
- they have read, understood and signed the staff/volunteer acceptable use agreement (AUA)
- understand and follow the procedures for reporting and recording online safety
- digital communications with children and families are professional and only carried out using the official systems of the setting.
- young people in their care are aware of online safety
- they are aware of current online safety trends and issues

Children

- are expected to abide by the acceptable use agreement/online safety rules
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should demonstrate positive online behaviours

Parents/carers

Parents/carers play a crucial role in supporting their children in the use of good online safety practice. *Parents/carers should sign the relevant permission forms as required.*

Practice

Taywood Nursery School and Extended Services has clear and effective procedures in place to manage online safety incidents for all users.

The use of technology is managed at the setting through:

- Supervision of children when online
- When internet is used, we manage access to online content through appropriate filtering
- Appropriate monitoring of system use
- Regular review of practice

We have clear lines of accountability and procedures are in place to identify, manage and escalate incidents when they arise. All staff/volunteers are aware of and implement these procedures.

Staff are aware of how to keep children safe.

Taywood Nursery School reviews it's practice regularly, informed by best practice and emerging threats through the use of improvement tools e.g. 360earlyyears.org.uk

Safeguarding

Online safety policy and practice in our setting meets requirements as defined in UK Law and statutory requirements.

Our online safety procedures are consistent with our wider safeguarding strategy.

We record and regularly analyse incidents to identify trends ensuring that safeguarding is effective and fit for purpose.

People

Educating children

Children need help and support to recognise and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

- key online safety messages will be reinforced as part of all relevant planned programmes of activities
- online safety issues will be discussed, when possible, in informal conversations with children
- when the opportunity arises, children will be guided to understand that not everything on the internet is true or accurate

We will provide online safety information and awareness to parents and carers through:

- letters, newsletters, website.
- meetings with parents/carers (formal and informal).
- providing links to relevant good practice information/websites for parents/carers
- involving families in celebrating online safety events e.g. Safer Internet Day

- making the setting's policies and resources accessible to parents/carers to encourage safe and responsible practice at home
- canvass parental views when developing policy

Training Adults

It is essential that all staff and volunteers receive online safety awareness training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of training about online safety will be made available to staff/volunteers.
- all new staff and volunteers will receive awareness training as part of their induction programme, ensuring that they fully understand the online safety policy and practice
- an audit of the online safety training needs of all staff will be carried out regularly
- the Online Safety Lead will be provided with opportunities to keep up to date with current online safety trends
- the Staff Online Safety Lead will provide advice/guidance/training to staff/volunteers as required
- this online safety policy and its updates will be presented to and discussed by staff/volunteers at staff/team meetings.

Personal Data

Data Protection

At Taywood Nursery School, personal data is recorded, processed, transferred and made available according to the current data protection legislation.

Our Setting

- has a Data Protection Policy
- implements the data protection principles and is able to demonstrate this through use of policies, notices and records
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO- Joanne Clegg)
- we know and record what personal data we hold, where this data is held, why and which member of staff/volunteer has responsibility for managing it
- we gain consent to obtain, store and process personal data from families, staff and volunteers and identify the more sensitive information classed as special category data

- will hold only the minimum personal data necessary to enable us to perform our function and will not hold that data for longer than necessary for the purposes for which it was collected
- will report any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law
- provides staff/volunteers and parents/carers with information about how we look after their data and what their rights are in a clear Privacy Notice
- ensures procedures are in place to deal with the individual rights of the data subject, e.g. subject access requests
- ensures Data Protection Impact Assessments (DPIA) are carried out where necessary.
- has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed
- understands how to share data lawfully and safely with other relevant data controllers
- ensures that all staff/volunteers receive data protection training at induction and appropriate refresher training thereafter
- ensures staff/volunteers:
    - take care to ensure the safekeeping 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 setting
    - will not transfer any setting personal data to personal devices

Responding to Issues

Taywood Nursery School can recognise online safety issues when they arise and there is clear guidance and established procedure to respond to them.

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is banned from any setting. Other activities e.g. promotion of terrorism or extremism are also banned and could lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in the context of the care of children, either because of the age of the users or the nature of those activities.

Our setting believes that the activities referred to in the following section would be inappropriate in a context of working with young children. The setting policy restricts certain internet usage and this is defined in the summary table “User Actions for Unsuitable/Inappropriate Activities” in the appendix to this policy.

Taywood Nursery School has clear and manageable procedures when dealing with misuse. They are dealt with quickly and proportionately and are recorded and well communicated. Where illegal misuse has been identified, it is immediately reported to the DSL/ Deputy DSL and escalated through the setting's safeguarding procedures to the appropriate supporting agency.

Our response is defined and guided by the "Online Safety Incident Flowchart" in the appendix to this policy.

Where we suspect that misuse might have taken place, but that the misuse is not illegal, we will investigate, preserve evidence and protect those carrying out the investigation. In such an event, we follow the guidance outlined in "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" *table in the appendix to this policy.*

Incidents of misuse by staff/volunteers will be dealt with through agreed disciplinary procedures as defined in the table "Disciplinary Actions: staff incidents" in the appendix to this policy.

Taywood Nursery School has a range of ways for our community to report online safety issues to us.

These include:

- nominated contact/person
- email
- parent messaging app- School Spider
- contact form on social media or web

We will respond to and act upon reports following the procedures described above. Outcomes from these will be used to inform and improve online safety policy and practice.

Technology

Devices

Technology is an intrinsic part of day-to-day operations in our setting and is used in many valuable ways to contribute to the work of our setting. We use:

- administrative computers
- laptops
- tablets

We monitor the use of these devices and how they are used through:

- supervision
- technical monitoring
- regular audit

We issue clear guidance for staff/volunteers and visitors on the use of personal mobile devices within our setting through:

- Clear acceptable use agreements acknowledged by staff/volunteers
- Clear rules and guidance for visitors on the use of personal mobile devices within our setting
- Rules and guidance on the use of devices displayed at sign in for visitors
- Clear signage in mobile-free areas of our setting

We encourage all of our community to feel confident in challenging device misuse when they identify it and to report it to us in the usual way. Our staff are instructed to not use personal devices for their professional role e.g. contacting parents/families; taking images/video; personal details of setting users etc.

Security

Taywood Nursery School has effective systems in place to ensure the security of devices, systems, images and personal devices. These are regularly reviewed and updated, in the light of constantly changing technology and new online security threats.

We have identified those devices and networks that are vulnerable to theft or their contents being compromised and have ensured they are both secure and protected, both physically and technically. We do this through:

- Having the latest operating system security updates installed
- Regularly updated antivirus and malware protection on all devices
- Protection from theft, loss or physical attack
- Data being regularly and securely backed up and stored on a secure cloud service
- Any removable media containing personal or sensitive data (e.g. *USB sticks or devices that leave our setting*) is secured through password and/or encryption

All devices and networks used professionally can only be accessed through secure passwords assigned to individual appropriate users. This allows us to manage and identify who has access to our systems.

All of our staff/volunteers are regularly trained and updated in the secure use of the devices we use in our setting.

If and when our staff/volunteers or children use the internet, we have ensured its use is safe and appropriate. We have:

- Blocked access to illegal content on our systems through filtering and regularly test its effectiveness e.g. using SWGfL Test Filtering site. At Taywood, Netsweeper is our filtering provider
- Ensured staff/volunteers only have access to appropriate agreed content on our systems through appropriate access and filtering
- Ensured appropriate access to online content used by children through supervision, filtering and the use of child friendly search engines e.g. SWGfL Swiggle
- Effective monitoring in place to alert us to any illegal access or misuse of our systems

Digital Images

Taywood Nursery School uses digital images and video as a tool to record and inform families/parents/carers of the progress and activities of their children. The devices we use for recording images of children are provided by the setting for staff/volunteers to use professionally.
We gain written permission from parents/carers/families to record and use digital image and video of their children. Through this process, we respect their rights under the Data Protection Act 2018.

Staff/volunteers are aware of the safeguarding risk to children if the privacy and security of those images is compromised and we have measures in place to limit this risk and to respond to issues when they arise.

Taywood Nursery School stores images securely and we meet legal requirements on how long we retain those images.

We share images with parents/carers and families through secure routes that include:

- Secure email
- Secure online platforms- School Spider
- Password-protected media

We publish clear guidance for parent'/carers' use and subsequent sharing of digital image/video that has been taken at the setting or at an event organised by the setting (particularly if other children are included).

We have processes in place to respond to parental concerns about how images are used and shared.

We ensure:

- care is taken that children are appropriately dressed in images
- that they are not participating in activities that bring the setting or its individuals into disrepute
- that full names of children are not shared on any public-facing media
- that children are educated to understand the risks of freely sharing images of themselves

Social Media and Communications

Our setting uses a range of online services to communicate with our community, that include:

- Website
- Social media pages
- Text messaging
- Closed messaging systems e.g. School Spider
- Email

All communications take place through clear and established setting systems and will be professional in nature.

Communications are monitored for concerns/complaints. There are clear processes in place to respond and resolve complaints or comments concerning our setting or staff/volunteers

All staff/volunteers have had clear, regularly updated guidance on their own use of personal media to protect their own professional role and the reputation of our setting.

Taywood Nursery School and Extended Services Acceptable Use Policy for Young Children

2023-2024

This is how we stay safe when we use computers:

- I will only use the computer/ interactive whiteboard that is for children
- I will only use activities that an adult has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer/interactive whiteboard

Signed (parent): ……………………………………….

Name of child: ……………………………………..

Date: ………………………………………………………..

Supporting Policy M2

Acceptable Use Agreement for Staff and Volunteers

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe online access at all times.

This Acceptable Use Agreement is intended to ensure that:

- staff and volunteers will act responsibly to stay safer while online, being a good role model for children.
- effective systems are in place for the online safety of all users and the security of devices, systems, images, and data.
- staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

The term "professional" is used to describe the role of any member of staff, volunteer or responsible adult.

For my professional and personal safety, I understand that:

- I will ensure that my on-line behaviours will be professional responsibilities, both to protect myself and the setting
- My use of technology could be monitored.
- When communicating professionally I will use the technology provided by the setting (e.g. official setting devices and technologies).
- I will not use my own personal devices using school WI-FI.
- I will not use school devices to access personal email addresses and social networking sites.
- These rules will apply when using the setting's technology either at home or away from the setting.
- If I need to use a school device at home (only SLT), I will not use the device for anything other than completing work (e.g. emails and one-drive).
- I will only use the setting's technology for personal use with permission (from Headteacher only)
- I will not take tablets home, as these contain images of children from the school day.
- I will delete images of children on school tablets once I have used them for photographic evidence (e.g. in school floor books.)

- I will not use school email accounts to register for social media sites or to sign up for promotions

For the safety of others:

- I will only access, copy, remove or otherwise alter other user's files, with permission
- I will communicate with others in a professional manner.
- I will only share other's personal data with their permission.
- I understand that any images I publish will be with the owner's permission and follow the setting's code of practice.
- I will only use the setting's equipment to record images of children.

For the safety of the group, I understand that:

- I will only access materials and content that are legal and appropriate.
- I understand the setting's reporting procedures and will immediately report any illegal, harmful or inappropriate incident.
- I will protect my online personal information (e.g. social networking profiles) to prevent access by the setting's children and families.
- I will respect and follow any systems designed to keep the group safer.
- I will only transport, hold, disclose or share personal information as outlined in the setting's Personal Data Policy. Where personal data is transferred externally, it will be password protected/encrypted.
- any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the setting's policy to disclose such information to an appropriate authority.
- personal passwords and those of other users should always be confidential.
- I will only download content that I have the right to use.
- I will only use my personal device/technology within the setting if I have permission and use it within the agreed rules
- I will inform the appropriate person if I find any damage or faults with technology.
- I will only install programmes on the systems devices belonging to the group, with permission

Staff / Volunteer Name

Signed

Date

This form will be printed and stored in the HT office.
Only the HT will have access to this form and will only share with the appropriate bodies on request (Ofsted/governors)
This form will be stored for one year and will be destroyed appropriately.

Consent Form for Parents and Carers

A copy of the Children's Acceptable Use Policy is attached to this permission form, so that parents/carers will be aware of the setting's expectations of the children in their care.

Parent/Carers Name:

Name of Child

As the parent/carer, I give permission for my child to use Taywood Nursery School's technology and devices.

I know that the setting has made my child aware of the *Acceptable Use Agreement* and has received guidance to help them understand the importance of online safety.

I understand that the setting will take reasonable precautions to ensure that my child will be safer when online, however, I understand that this manages risk but cannot eliminate it.

I understand that my child's online activity will be supervised and monitored and that the setting will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I understand that the setting will take appropriate action in the event of any incidents.

I will encourage my child to adopt safe use of online technologies.

Signed Date

Use of Digital/Video Images

The use of digital/video images plays an important part in our activities. Children, staff and volunteers may use devices to record images/evidence of those activities. These images may then be used in Floor Books and presentations and may also be used to celebrate success through their publication in newsletters, on the website and occasionally in the public media.

The setting will comply with the Data Protection Act and request parent's/carers permission before taking images of their children. We will also ensure that, wherever possible, full names will not be published alongside images.

It's a great thing to film your child at our events and we know they provide a lot of precious memories. You can support us in keeping the children safe by considering the following:

- Images and video should be for your own or family's personal use only
- Think about privacy and who has the right to see your images, not only of your own child but of others
- If you do share the images online, then you must make sure they are limited to immediate family only and are not made public
- If you need help in knowing how to do this, then come and have a chat with us

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

Permission Form

Parent/Carers Name

Name of Child

As the parent/carer of the above child, I agree to the group taking and using digital/video images of my child/children. I understand that the images will only be used to support legitimate activities or in publicity that reasonably celebrates success and promotes the work of the group.

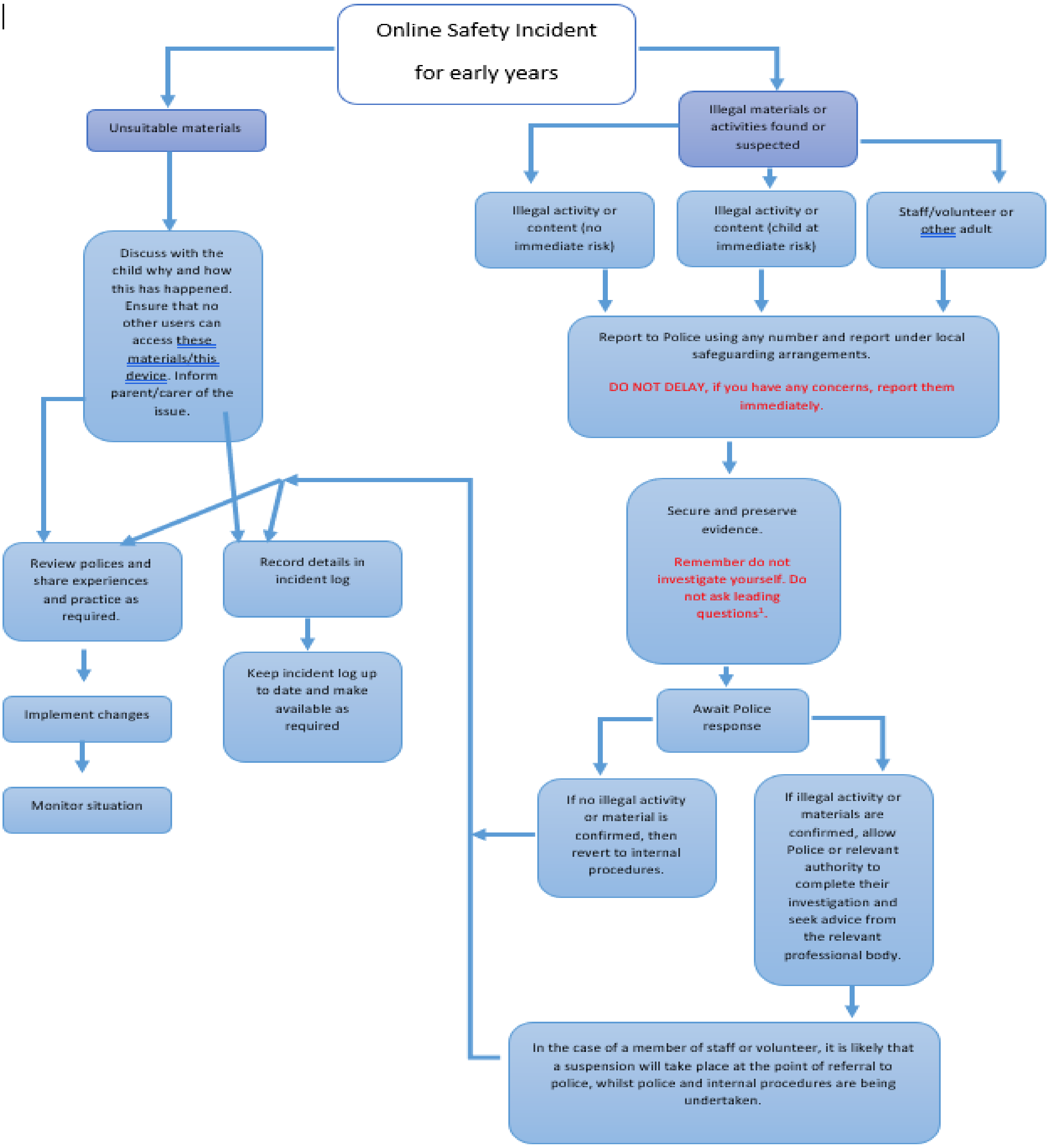
I agree that if I take digital or video images at group events, they will not include images of other children, other than my own, unless I have the permission of their parent and I will abide by these guidelines in my use of the images.

Signed Date

This form will be stored in a paper copy in the school office.
Only SLT and the school office staff will have access to this form.
It will be stored until the child leaves Taywood Nursery School.
It will be destroyed appropriately at this point.

Flowchart for responding to online safety incidents

Supporting Policy P2



Online Safety Incident for early years

Unsuitable materials

Discuss with the child why and how this has happened. Ensure that no other users can access these materials/this device. Inform parent/carer of the issue.

Review polices and share experiences and practice as required.

Implement changes

Monitor situation

Record details in incident log

Keep incident log up to date and make available as required

Illegal materials or activities found or suspected

Illegal activity or content (no immediate risk)

Illegal activity or content (child at immediate risk)

Staff/volunteer or other adult

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Unsuitable / Inappropriate Activities

This section should be used in conjunction with the Acceptable Use Policy November 2023

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not 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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the					X

	Criminal Justice and Immigration Act 2008					
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the setting or brings the setting into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						X

• Gaining unauthorised access to setting networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the setting				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using setting systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce			X		

File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

Guidance for Reviewing Internet Sites (for suspected harassment and distress)

This guidance is intended for use when settings need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include online-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case, please refer to the Flowchart for responding to online safety incidents and report immediately to the police

Please follow all steps in this procedure:

- Have more than one senior leader/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by children and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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, signed and attached to the form (**except in the case of images of child sexual abuse – see below**)
- Once this has been completed and fully investigated the group 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 Local Authority or national / local organisation
- Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- incidents of 'grooming' behaviour
- the sending of obscene materials to a child

- Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Record of reviewing internet sites (for suspected harassment / distress)

Group	
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

Web site(s) address	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Reporting Log Group ………………. ………………. ……………….	Signature									
	Incident Reported by									
	Action taken	By whom?								
		What?								
	Incident									
	Time									
	Date									

Disciplinary actions

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Setting Leader	Refer to Local Authority /HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities - Appendix P3).		X	X	X				
Inappropriate personal use of the internet/social media/personal email		X	X	X				
Unauthorised downloading or uploading of files		X						
Unauthorised access to the setting network/devices		X			X	X		
Careless use of personal data e.g. holding or transferring		X	X			X		

data in an insecure manner								
Deliberate actions to breach data protection or network security rules		X	X			X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X			X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X	X	X
Using personal devices/accounts to communicate with children		X	X	X		X	X	X
Actions which could compromise the staff/volunteer's professional standing		X	X			X	X	
Actions which could bring the setting into disrepute		X	X			X	X	X
Subvert the setting's filtering system		X	X		X			
Accidentally accessing		X	X		X	X		

offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X				X	X	
Continued infringements of the above, following previous warnings		X	X			X	X	X

Training Needs Audit

Training Needs Audit Log Group .... Date	Review date								
	Cost								
	To be met by:								
	Identified training need								
	Relevant training in last 12 months								
	Position								
	Name								

Supporting Policy P7

Setting Personal Data Advice and Guidance

Important note:

This document is for advice and guidance purposes only. It is anticipated that settings will use this advice alongside their own data protection policy. This document is not intended to provide legal advice and the setting is encouraged to seek their own legal counsel when considering their management of personal data.

Data Protection Law – A Legislative Context

In 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

Does the Data Protection Law apply to Early Years settings?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a 'data controller'. Personal data is information that relates to an identified or identifiable living individual (a data subject). Guidance for settings is available on the Information Commissioner's Office (ICO) website including information about the Data Protection Law.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to data subjects;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the setting to put in place appropriate privacy notices (to give a data subject information about the personal data processing activities, lawful basis of processing and individual rights) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

Data Mapping to identify personal data, data subjects and processing activities

The setting and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the setting may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the setting has a data map of these activities; it can then make sure that the correct privacy notices are provided, put in place security measures to keep the personal data secure and other steps to avoid breach and also put in place data processing agreements with any third parties.

The data map should identify what personal data held in digital format or on paper records in a setting, where it is stored, why it is processed and how long it is retained. A typical data map may include:

- Parents/carers – names, addresses, contact details
- Children - lists, learner progress records, reports, references, contact details, health and SEN reports
- Staff/volunteers and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

Some types of personal data are designated as 'special category' being personal data;
"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

This should be identified separately and to lawfully process special category data, you must identify both a lawful basis and a separate condition for processing special category data. You should decide and document this before you start processing the data.

The setting will need to identify appropriate lawful process criteria for each type of personal data:

1. Consent: the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance)
2. Contract: the processing is necessary for a contract you have with the data subject
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Consent has changed as a result of the GDPR and is now defined as: "in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

This means that where a setting is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but settings should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to use consent as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it's important that you only use consent for optional extras, rather than for core information the setting requires in order to function. Examples;

- ➢ consent would be appropriate for considering whether a child's photo could be published in any way.

- if your school or academy requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- Who the controller of the personal data is
- What personal data is being processed and the lawful purpose of this processing
- where and how the personal data was sourced
- to whom the personal data may be disclosed
- how long the personal data may be retained
- data subject's rights and how to exercise them or make a complaint

In order to comply with the fair processing requirements in data protection law, the setting will inform parents/carers of the data they collect, process and hold on the children, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed.

Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it
- to restrict processing – blocking or suppression of processing
- to portability – unlikely to be used in a setting context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

A setting must not disclose personal data even if requested in a Subject Access Request;

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs

Breaches and how to manage a breach

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue. It is important that the setting has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

All significant data protection incidents must be reported through the DPO to the Information Commissioner's Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

The setting should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- "responsible person" for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising

Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts (and re-visit it annually)

The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

You could ask these simple questions:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') you are using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

Secure storage of and access to data

The setting should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Staff/volunteers will not, as a matter of course, be granted access to the whole management information system.

Good practice suggests that all users will use strong passwords. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on setting equipment. Private equipment (i.e. owned by the users) must not be used for the storage of setting personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with setting policy once it has been transferred or its use is complete.

The setting will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The setting should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on setting systems, including off-site backups.

The setting should have clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. As a Data Controller, the setting is responsible for the security of any data passed to a "third party". Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

Secure transfer of data and access out of the Early Years setting

The setting recognises that personal data may be accessed by users out of setting or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the setting or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of setting
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

Disposal of personal data

The setting should implement a document retention schedule that defines the length of time personal data is held before secure destruction. The setting must ensure the safe destruction of personal data when it is no longer required. A Destruction Log should be kept of all data that is disposed of.

Demonstrating Compliance - Audit Logging / Reporting / Incident Handling

Organisations are required to keep records of processing activity. Records must include:

- the name and contact details of the data controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures

Clearly, in order to maintain these records good auditing processes must be followed.

Fee

The setting should pay the relevant annual fee to the Information Commissioner's Office (ICO). Failure to renew may render the setting to a penalty in addition to other fines possible under the Data Protection Law.

Responsibilities

Every maintained setting is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

They must have:

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level

The data controller must:

1. not give the DPO instructions regarding the performance of tasks
2. ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
3. not dismiss or penalise the DPO for performing the tasks required of them

As a minimum a Data Protection Officer must:

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with Data Protection Law

Everyone in the setting has the responsibility of handling protected or sensitive data in a safe and secure manner.

Training & awareness

All staff/volunteers must receive data handling awareness / data protection training and will be made aware of their responsibilities.

Parental permission for use of cloud hosted services

Settings that use cloud hosting services are advised to seek appropriate consent to set up an account for learners.

Supporting Policy T1

How we use technology to communicate

The following table shows how this setting currently considers the benefit of using these technologies outweighs their risks / disadvantages:

	Staff/volunteers				Children			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff / volunteers	Not allowed	Allowed	Allowed at certain times	Allowed with staff / volunteers permission	Not allowed
Mobile phones in the staff room and office spaces	X							X
Taking photos on personal mobile phones, tablets or cameras				X				X
Taking photos on school tablets and cameras	X				X			
Use of hand held devices e.g. gaming consoles				X				X
Use of the organisation's email for personal emails				X				
Personal use of online communication technologies e.g. social networking, messaging, email				X				X

Setting Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Our setting will be responsible for ensuring that systems and devices are as safe and secure as is reasonably possible and that:

Responsibilities

The management of technical security will be the responsibility of Mrs. Jennifer Slater (Headteacher)

Policy statements

We will be responsible for ensuring that our systems and devices are as safe and secure as is reasonably possible and that policies and procedures are implemented. We will also ensure that staff and volunteers receive guidance and training and effectively carry out their responsibilities:

- we regularly review and audit the safety and security of our technical systems
- our servers, wireless systems, cabling and devices are securely located and physical access is restricted to deter theft, loss or physical attack
- appropriate technical security measures are in place to protect the following from accidental or malicious online attempts to threaten our technical security
- *servers*
- *firewalls*
- *switches*
- *routers*
- *wireless systems*
- *devices*
- *computers*

- the setting's systems and devices are protected by up to date software to protect against malicious threats from viruses and malware etc.
- the responsibility for the management of technical security is clearly assigned to appropriate staff (Headteacher and Bursar)

- all users will have clearly defined access rights to our systems and devices.
- users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion of security breaches
- our data is regularly backed up *and stored off-site or on a secure cloud service*
- we ensure that all our software licences are accurate and up to date
- we will regularly monitor and record the activity of users on the setting technical systems and users are made aware of this in the acceptable use agreement
- we have an appropriate system in place for users to report any actual/potential technical incident (through the school office and Lancashire Digital Services)
- our users can only download programmes with appropriate permission
- staff/volunteers understand our policy regarding the use of removable media/devices (e.g. memory sticks/storage devices/laptops) removed offsite

Password Security

Policy Statements:

- our systems and devices are protected by secure user passwords
- relevant staff/volunteers will be provided with a username and password by Mrs. Jennifer Slater (Headteacher) and Mrs. Joanne Clegg (Bursar) who will keep an up to date record of users and their usernames.
- Our staff/volunteers are responsible for the security of their username and password, must not share them or allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Password requirements:

- Passwords should be long. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of setting
- Passwords must not include names or any other personal information about the user that might be known by others

- Passwords should be changed on first login to the system
- An administrator account password for the setting systems should be kept in a secure place e.g. a safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.

Filtering and Monitoring

Introduction

Where a setting has access to the internet, the filtering of content provides an important means of preventing users from accessing material that is illegal or managing access to relevant or inappropriate content. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed.

It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the setting has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the setting.

Settings may wish to test their filtering for protection against illegal materials at SWGfL Test Filtering

Responsibilities

The responsibility for the management of the setting's filtering policy will be held by Mrs. Jennifer Slater as Headteacher, but delegated to Mrs. Joanne Clegg (Bursar). They will manage the setting filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to Joanne Clegg any infringements of the setting's filtering policy of which they become aware and/or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

- Our Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the setting.
- Illegal content is filtered by our broadband/filtering provider by actively employing the Internet Watch Foundation CAIC list; the Home Office Approved List for Terrorist Content (CTIRU) and other illegal content lists.
- We ensure appropriate access to online content used by children through supervision, filtering and the use of child friendly search engines e.g. SWGfL Swiggle
- Filter content lists are regularly updated and internet use is logged and monitored.
- The monitoring process alerts the setting to breaches of the filtering policy, which are then acted upon.
- Any filtering issues should be reported immediately to Joanne Clegg.
- Requests from staff/volunteers for sites to be removed from, or added to, the filtered list will be considered and recorded by Joanne Clegg and requested through LCC Digital Services.

Education/Training/Awareness

Staff/volunteers are made aware of the technical security policy/passwords/filtering through:

- the acceptable use agreement and technical security policy
- induction training
- staff/volunteer meetings
- communications updates

Parents are informed of the setting's filtering policy through the acceptable use agreement

All users (including children) are encouraged to report any concerns they might have when engaging in online activities.

Further Guidance

Settings in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in setting, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).

The Department for Education 'Keeping Children Safe in Education' requires settings to: "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the setting or colleges IT system" however, settings will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

In response UKSIC produced guidance on – information on "Appropriate Filtering"

SWGfL provides a site for settings to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

Supporting Policy T3

Monitoring Log

Monitoring Log Group …………………… ……………………	Signed								
	Reported to								
	Issues identified								
	Monitored by								
	Programme / Services Monitored								
	Date								

Mobile Technologies Policy (Inc. BYOD/BYOT)

Mobile technology devices may be a setting owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that has the capability of accessing the setting's wireless network.

Staff/volunteers will be reminded that the primary purpose of having their personal device at the setting is professional and that this is irrespective of whether the device is setting owned/provided or personally owned.

Considerations

We understand that there are a number of issues and risks to consider when implementing the use of mobile technologies, these include; security risks in allowing connections to the setting network, filtering of personal devices, breakages and insurance, access to devices, avoiding potential distraction, network connection speeds, types of devices and charging facilities.

Our setting allows the use of mobile technologies as follows:

- The setting acceptable use agreements for staff/volunteer, children, parents/carers and visitors will give consideration to the use of mobile technologies
- The setting allows:

	setting/devices			Personal devices		
	setting owned and allocated to a single user	setting owned for use by multiple users		Family owned	staff/volunteer owned	Visitor owned
Allowed in setting	Yes	Yes		Yes/No	Yes/No	Yes/No
Full network access	*Yes*	*Yes*				
Internet only						
No network access				Yes	Yes	Yes

We have provided technical solutions for the safe use of mobile technology for setting devices/personal devices.

- all setting devices are controlled through appropriate Mobile Device Management software
- appropriate access control is applied to all mobile devices (e.g. Internet only access, network access allowed, shared folder network access)
- we have sufficient broadband performance and capacity to ensure our core activities will not be affected by the increase in the number of connected devices
- for all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- appropriate exit processes are implemented for devices no longer used at a setting location or by an authorised user or when a user leaves the setting.
- all setting devices are subject to routine monitoring
- When personal devices are permitted:
- we have technical solutions in place to provide appropriate levels of network access
- personal devices are brought into the setting entirely at the risk of the owner, including the liability for any loss or damage resulting from the use of the device in setting
- we recommend that insurance is purchased to cover that device whilst out of the home
- we accept no responsibility for any malfunction of a device due to changes made to the device while on the setting network or whilst resolving any connectivity issues
- we recommend that the devices are made easily identifiable.
- pass-codes or PINs must be set on personal devices to aid security
- we are not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements
- visitors will be provided with information about how, when and where they are permitted to use mobile technology in line with local safeguarding arrangements
- users are responsible for keeping their device up to date through software, security, anti-virus protection and app updates.
- users are responsible for charging their own devices and for protecting and looking after their devices while in the setting
- devices must be in silent mode on the setting site
- users must have permission to change settings or add/delete programmes/apps to setting devices.
- users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- users must only take photos of people with their consent.

- staff/volunteer owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- printing from personal devices is not permitted
- personal devices should be charged before being brought to the setting as the charging of personal devices is not permitted during the setting day

Social Media Policy

Social media (e.g. Facebook, Twitter, Instagram, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other online. However, some games, for example Minecraft or Roblox and video sharing platforms such as You Tube or TikTok have social media elements to them.

The setting recognises the numerous benefits and opportunities which a social media presence offers. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and reputation. This policy aims to encourage the safe use of social media by the setting, its staff/volunteers, children and families.

Scope

This policy is subject to the setting's codes of conduct and acceptable use agreements.

This policy:

- Applies to all staff/volunteers and to all online communications which directly or indirectly, represent the setting.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the setting

We respect privacy and understand that staff/volunteers may use social media in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the setting's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on an approved setting account or using the setting name. All professional communications are within the scope of this policy.

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 setting, it must be made clear that the member of staff is not communicating on behalf of the setting with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the setting are outside the scope of this policy.

Roles & Responsibilities

Leaders

- will ensure that training and guidance is available for staff/volunteers and education for the children
- will develop and implement the Social Media policy
- will take a lead role in investigating any reported incidents
- will approve any social media sites established by the setting.
- will monitor relevant social media and communications

Administrator/Moderator

- will create and securely manage accounts following leader's approval
- will be involved in monitoring and contributing to the account

Staff

- will understand that any use of social media is carried out in line with this and other relevant policies
- will receive relevant training and guidance

Process for creating setting accounts

Setting social media accounts will only be created following discussion about:

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Leaders will need to be satisfied that anyone running a social media account on behalf of the setting has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the setting, including volunteers or parents.

Monitoring

Setting accounts will be monitored regularly and frequently to prevent bullying; abuse of staff or any other inappropriate behaviour on a setting social media account.

Behaviour

- all users using social media are required to adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff will be professional and respectful at all times and in accordance with this policy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are not allowed on setting accounts
- If a journalist makes contact about posts made using social media staff must follow the setting media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the setting and will be reported as soon as possible to a leader and escalated where appropriate. (further support is available at SWGfL Report Harmful Content)
- We permit reasonable and appropriate access to private social media sites during break periods and when away from the children. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The setting will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the setting will deal with the matter internally. Where conduct is considered illegal, the setting will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users must ensure that their use of social media does not infringe upon relevant data protection laws (see appendix on Data Protection), or breach confidentiality.

Handling abuse

- If a conversation turns and becomes offensive or unacceptable, setting users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed setting protocols.

Tone

The tone of content published on social media will be appropriate to the audience and professional in nature.

Use of images

- **permission to use any photos or video recordings should be sought in line with our setting's digital and video images policy.** If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student/pupil pictures online other than via setting owned social media accounts**
- Staff/volunteers will exercise their professional judgement on whether an image is appropriate to share on setting social media accounts. Children should be appropriately dressed, not be subject to ridicule and must not be on any setting list of children whose images must not be published.

Personal use

Staff

- Personal communications are those made via a personal social media account. If the setting is referred to in, or associated with, a post on a personal account, it must be made clear (with an appropriate disclaimer) that the member of staff/volunteer is not communicating on behalf of the setting. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the setting are outside the scope of this policy.
- *We permit reasonable and appropriate access to private social media sites in the setting, but disciplinary action may be taken if this is excessive or inappropriate.*

Children

- **Staff/volunteers are not permitted to follow or engage with current or prior children/families from the setting on any personal social media network account.**
- We will use relevant opportunities in our education programmes to encourage children be safe and responsible users of social media.

Parents/Carers

a) When parents/carers have access to our setting platforms/accounts (e.g. School Spider), they will be informed about acceptable use.

b) *The setting has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.*
c) *Our parents/carers are encouraged to comment or post appropriately about the setting. In the event of any offensive or inappropriate comments being made, we will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, we will refer parents to the setting's complaints procedures.*

Monitoring posts about the setting

1. We will monitor social media for public postings about the setting. (SWGfL Reputation Alerts can assist you in this process)
2. We will respond to social media comments made by others according to our defined policies and processes.

Further guidance

Managing your personal use of Social Media:

- Very little on social media is truly private
- Social media can blur the lines between your professional and private life. Don't make references to the setting on personal accounts
- Check your settings regularly and test your privacy. Check app permissions within your privacy settings to reduce the amount of personal information that "bleeds" from your account use.
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider: scale, audience and permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents/carers say about you if they could see your images?
- Know how to report a problem to your social media provider. Get extra advice and support from Report Harmful Content service at https://reportharmfulcontent.com

Managing setting social media accounts

The Do's

- Check with your setting leader before publishing content that may have controversial implications for the setting

- Use a disclaimer when expressing personal views. Some examples are illustrated at FreePrivacyPolicy.com
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the setting's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the setting into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of setting accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Links to other organisations or documents

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

UK Safer Internet Centre

Safer Internet Centre – saferinternet.org.uk

South West Grid for Learning - swgfl.org.uk/products-services/online-safety

Child net – childnet-int.org

Professionals Online Safety Helpline - saferinternet.org.uk/about/helpline

Internet Watch Foundation - iwf.org.uk

Report Harmful Content - reportharmfulcontent.com

Other

CEOP - ceop.police.uk

Common Sense Media

Vodafone - Digital Parents Magazine

Get Safe Online

Internet Matters

UK Government / England guidance

Early Years guidance - Safeguarding children and protecting professionals in early years settings: online safety considerations

DfE – Keeping Children Safe in Education

Ofsted - Education Inspection Framework

UK Government - Working Together to Safeguard Children

UKCIS - UK Council for Internet Safety

UKCIS - Safeguarding children and protecting professionals in early years settings: online safety guidance for managers

UKCIS - Education for a Connected World

UKCIS - Digital Resilience Framework

PREVENT - Prevent duty guidance for England, Scotland and Wales

Safer Recruitment Consortium - Guidance for safer working practice for adults that work with children and young people

Management

Tools

Early Years Toolkit - early years toolkit

Online Safety BOOST – boost.swgfl.org.uk

SWGfL Test filtering - testfiltering.com

People

Educating Children

SWGfL Evolve - projectevolve.co.uk

UKCIS – Education for a connected world framework

Childnet - Digiduck

Childnet - Digital wellbeing - guidance for parents

UKSIC - Safer Internet Day

ThinkUKnow - thinkuknow.co.uk

PACEY - Online Safety

Internet matters - Early years resources

Training Adults

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

SWGfL Online Safety Training - swgfl.org.uk/training/online-safety-training

SWGfL BOOST Online Safety Training Programme - swgfl.org.uk/products/online-safety-boost

Data Protection

ICO - Guide to data protection

ICO - Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

SWGfL - GDPR guidance for schools and colleges

PACEY - record keeping fact sheet

PACEY - GDPR guidance

Responding to issues

SWGfL - Whisper Anonymous Reporting App

Technology

UKSIC – Appropriate Filtering and Monitoring

SWGfL - Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Social Media

UKSIC - Safety Features on Social Networks

Children's Commissioner - Young peoples' rights on social media

Research

Ofcom – Media Literacy Research

UK Safer Internet Centre Education Research Digest

Legislation

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

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

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.

Data Protection Act 1998

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

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

The Data Protection Act 2018:

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

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.
- All data subjects have the right to:
- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

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.

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. 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. 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 setting is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Serious Crime Act 2015

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

Glossary of terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority

LAN Local Area Network

MIS Management Information System

NEN National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

Ofcom Office of Communications (Independent communications sector regulator)

SWGfL South West Grid for Learning Trust – the provider of online safety and security services for schools and other organisations. Lead partner in the UK Safer Internet Centre

TUK Think U Know – educational online safety programmes for schools, young people and parents.

UKSIC UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

UKCIS UK Council for Internet Safety

WAP Wireless Application Protocol more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework

Acknowledgements

SWGfL would like to acknowledge the contribution of a wide range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of the online safety policy templates and of the 360 degree safe online safety self-review tool.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in June 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.