

Online Safety Policy

SOUTH NORMANTON NURSERY SCHOOL

Adopted at the meeting of the Full Governing Body on **8th October, 2024**

Minute Number

Chair of Governors

Record of Policy Amendment / History

Version	Date	Author	Reason for Change
V1	21.09.21	SWGfL/RD	Amendments, additions and contextualisation are in yellow.
V2	24.09.24	SWGfL/MH	SWGfL document reviewed September 2023 Amendments, additions and contextualisation are in yellow.

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

Version: 2

Date created: 24/09/24

Next review date: 07/10/25

Contents

Scope of the Online Safety Policy	2
Policy development, monitoring and review	2
Schedule for development, monitoring and review	3
Process for monitoring the impact of the Online Safety Policy	3
Policy and leadership.....	4
Responsibilities	4
Professional Standards	8
Policy.....	9
Online Safety Policy.....	9
Acceptable use.....	9
User actions.....	10
Reporting and responding	13
Online Safety Incident Flowchart	16
Responding to Learner Actions.....	17
Responding to Staff Actions.....	19
Online Safety Education Programme.....	20
Contribution of Learners	21
Staff/volunteers.....	22
Governors	22
Families	23
Adults and Agencies.....	23
Technology	23
Filtering & Monitoring.....	24
Filtering	24
Monitoring.....	25
Technical Security.....	25
Mobile technologies.....	27
Social media.....	28
Digital and video images	30
Online Publishing.....	31
Data Protection	32
Outcomes.....	34

This policy has been considered and written in conjunction with our Rights Respecting School's charter adapted from the United Nations Convention on the Rights of a Child.

'In our school, we believe that every child has the right to play, learn and grow in an inspiring, empowering and safe environment protected from harm and treated fairly. We believe that each one of us has a responsibility for the world and its inhabitants, both of which deserve respect and nurture.'

South Normanton Nursery School Charter

As silver status UNICEF Respecting Rights schools award holders, the whole school community is committed to upholding children's rights and the convention on the rights of the child is embedded within daily life at our school – this is especially around ensuring that children understand how to stay safe, recognise unsafe situations and know how to report if they are not safe.

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of **South Normanton Nursery School** to safeguard members of our school community online in accordance with statutory guidance and best practice. *Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.*

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

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

Policy development, monitoring and review

This online safety policy has been developed by

- Headteacher (*who is also the Online Safety Lead*)
- Governors

Schedule for development, monitoring and review

This Online Safety Policy was approved by the <i>school Governing Body</i> on:	<i>8th October, 2024</i>
The implementation of this Online Safety Policy will be monitored by:	<i>The Headteacher</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The <i>Governing Body</i> will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>As and when an incident occurs</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>7th October, 2025</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>LA Safeguarding Officer, LADO (Miles Dent), Police as appropriate</i>

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using: (delete/add as relevant)

- logs of reported incidents
- Filtering and monitoring logs (received weekly from Senso Alerting – reviewed by Headteacher)
- internal monitoring data for network activity (This is done by LEAD IT)
- surveys/questionnaires of:
 - parents and carers
 - staff.

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals¹ and groups within the school.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education. (the Lead DSL is the Headteacher)
- The Headteacher, Teacher, SBM and SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff².
- The Headteacher/SLT are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headteacher/SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Headteacher/SLT will receive regular monitoring reports from LEAD IT on request
- The Headteacher/SLT will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Weekly violation reports are received from Senso Alerting and reviewed by the Headteacher.

¹ In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.

² See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Body* (Governor for Safeguarding) has taken on the role of *Online Safety Governor*. The role of the Online Safety Governor will include **as part of Full Governors meetings and safeguarding monitoring:**

- **regular meetings with the Designated Safeguarding Lead / Online Safety Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.** (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible Governor) - in-line with the DfE Filtering and Monitoring Standards
- **reporting to the Full Governing Body**
- Receiving (at least) basic cyber-security training to enable the Governors to check that the school meets the DfE Cyber-Security Standards

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

Designated Safety Lead (DSL)

The **lead** DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety Governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant Governing Body meetings
- report regularly to the **SLT**
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

This is currently the Headteacher.

The Online Safety Lead will:

- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/Governors/parents/carers/learners
- liaise with LEAD IT technical staff
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
 - content
 - contact
 - conduct
 - commerce

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the Headteacher/DSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure pupils (supported by staff) understand and follow the Online Safety Policy and acceptable use policies as appropriate for their age

- only use pupil logons when children are using the internet. This is always supported by a staff member or in the case of programs accessed through the internet, the program is locked with password protection accessible only by staff members.
- work alongside children and directly supervise them to carry out research when using a staff log on. This is filtered for appropriate use.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Online safety is reinforced by all staff through stories which are planned throughout the year, a song, modelling and 'in the moment' discussions and praise to support relevant understanding.

A planned online safety curriculum should be provided throughout the year and is revisited when pertinent to learning in line with the children's selection of activities in nursery.

IT Provider **(LEAD IT)**

LEAD IT are responsible for ensuring:

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

Pupils:

- are responsible for using the **South Normanton Nursery School** digital technology systems in accordance with the Online Safety Policy. **Due to the age of our children, internet use and use of digital technology is always supported by an adult.**

- our children are taught at an age appropriate level through stories and 'in the moment' discussion and modelling about the potential dangers of digital technology and internet use, and how to use it safely. This is to support them as they develop their understanding and encourage them to share their concerns with staff and parents

Parents and carers

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

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

- publishing the school Online Safety Policy on the school website
<https://www.southnormantonnurseryschool.co.uk/online-and-personal-safety/>
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- digital and video images taken at school events. This is always discussed by the Headteacher prior to the event commencing
- access to parents' sections of the website/Learning Platform and on-line student/pupil records including Tapestry
- reinforcing the online safety messages provided to learners in school.

Community users

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

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Policy

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on the school website.

Acceptable use

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

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through: learner handbook

- staff induction and handbook
- school website

At South Normanton Nursery School, staff read and sign our IT Security and Acceptable Use Policy through My Concern.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	<p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering <p>N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges</p>					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) <p>N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here</p>					X

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

	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.								
Online gaming	X							
Online shopping/commerce				X				
File sharing				X				
Social media				X				
Messaging/chat	X				X			
Entertainment streaming e.g. Netflix, Disney+	X				X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok				X	X			
Mobile phones may be brought to school		X			X			
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school	X				X			
Taking photos on mobile phones/cameras				X	X			

Use of other personal devices, e.g. tablets, gaming devices	X				X			
Use of personal e-mail in school, or on school network/wi-fi	X				X			
Use of school e-mail for personal e-mails	X				X			

Social media refers to the nursery social media pages, the Headteacher, teacher and SBM only have access to upload to these sites.

Taking photos on mobile phones/cameras – the SBM will do this periodically to take photos of i.e. staff for ID badges. Images will be deleted AS SOON as they are emailed to the SBM's school email account.

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

- **when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.**
- **any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.** Personal e-mail addresses, text messaging or social media must not be used for these communications.
- **staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community**
- **users should immediately report to a nominated person (the Headteacher) – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- relevant policies (Social Media and IT Security and Acceptable Use) and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Reporting and responding

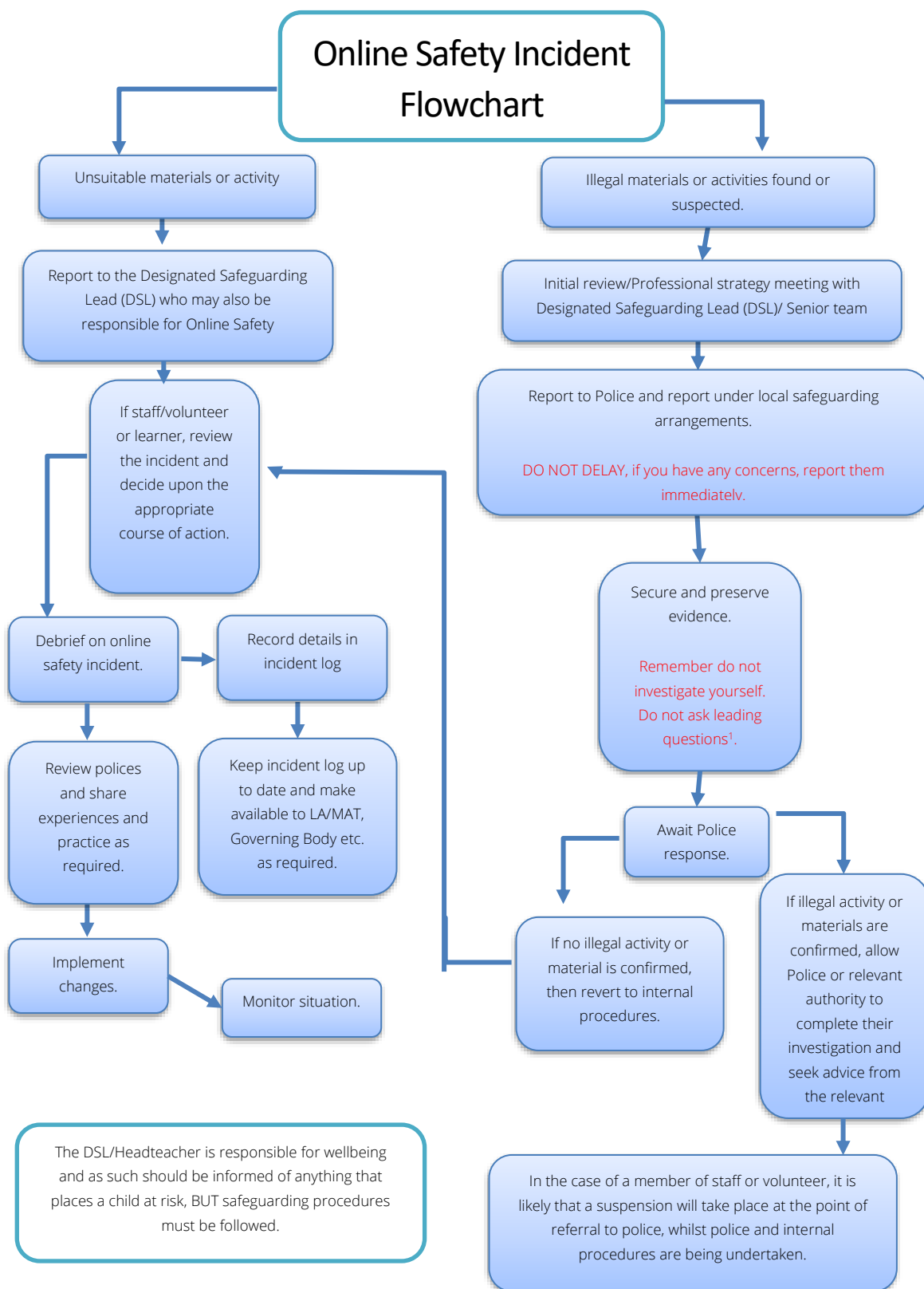
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- **there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**

- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm ([see flowchart and user actions chart in the appendix](#)), the incident must be escalated through the agreed school safeguarding procedures, this may include
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking [offences under the Computer Misuse Act](#)
 - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
- where there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
 - 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 (as relevant)
 - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged (see Appendix A3)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided to:
 - staff, through regular briefings
 - parents/carers, through newsletters, school social media, website
 - Governors, through regular safeguarding updates
 - local authority/external agencies, as relevant

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



School actions

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

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	n/a							
Corrupting or destroying the data of other users.	n/a							
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	n/a							
Unauthorised downloading or uploading of files or use of file sharing.	n/a							
Using proxy sites or other means to subvert the school's filtering system.	n/a							
Accidentally accessing offensive or pornographic material and failing to report the incident.	n/a							

Deliberately accessing or trying to access offensive or pornographic material.	n/a
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	n/a
Unauthorised use of digital devices (including taking images)	n/a
Unauthorised use of online services	n/a
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	n/a
Continued infringements of the above, following previous warnings or sanctions.	n/a

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a 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)		X	X	X				
Deliberate actions to breach data protection or network security rules.							X	
Deliberately accessing or trying to access offensive or pornographic material								X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software							X	
Using proxy sites or other means to subvert the school's filtering system.								X
Unauthorised downloading or uploading of files or file sharing		X						
Breaching copyright or licensing regulations.							X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X						
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature								X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers								X

Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X						
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		X						
Actions which could compromise the staff member's professional standing							X	
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.							X	
Failing to report incidents whether caused by deliberate or accidental actions		X						
Continued infringements of the above, following previous warnings or sanctions.								X

Online Safety Education Programme

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. Online safety is reinforced by all staff through stories which are planned throughout the year, a song, modelling and 'in the moment' discussions and praise to support relevant understanding.

A planned online safety curriculum should be provided throughout the year and is revisited when pertinent to learning in line with the children's selection of activities in nursery.

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A **planned online safety curriculum** for all year groups matched against a nationally agreed framework e.g. **Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve** and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through **effective planning and assessment**
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#)

- **the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.**
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the [CyberChoices](#) site.*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*
- **the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.**

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through: [\(amend as relevant\)](#)

- *mechanisms to canvass learner feedback and opinion.*
- *appointment of digital leaders/anti-bullying ambassadors/peer mentors [\(or similar groups\)](#)*
- *the Online Safety Group has learner representation*
- *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
- *learners designing/updating acceptable use agreements*

- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.*

Staff/volunteers

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

- **a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**
- **the training will be an integral part of the school's annual safeguarding and data protection training for all staff**
- **all new staff will receive online safety training as part of their induction programme, given by the Headteacher, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to ent, professional conduct, online reputation and the need to model positive online behaviours.**
- the Online Safety Lead will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

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

- attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or

A higher level of training will be made available to the Online Safety Governor. This will include:

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

Families

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

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

- letters, newsletters, web site, Tapestry.
- parents/carers evenings/sessions, timely discussions where appropriate.
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carers evenings.*
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. *Safer Internet Day*
- reference to the relevant web sites/publications *which are linked on our website*
<https://www.southnormantonnurseryschool.co.uk/helpful-links-to-support-online-safety/>.
- *Sharing good practice with other schools in clusters and or the local authority/MAT*

Adults and Agencies

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

- the South Normanton Nursery School website provides online safety information accessible to the wider community. Safety information shared on our website and via social media is relevant to older children and families also, thus supporting the wider community.
- sharing their online safety expertise/good practice with other local schools and Childminders to enhance their online safety provision.

Technology

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

Filtering & Monitoring

The school filtering and monitoring provision is agreed by SLT, Governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. **Violation monitoring reports are received weekly through Senso Alerting.**

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider **(Lead IT)** will have technical responsibility

The filtering and monitoring provision is reviewed (at least annually) by SLT, the Designated Safeguarding Lead and a Governor with the involvement of the IT Service Provider.

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

Filtering

- the school manages access content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre [Appropriate filtering.](#)
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- **there is a clear process in place to deal with, and log, requests/approvals for filtering changes (these requests are directed to Lead IT)**
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- younger learners will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](#)
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- the school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. [These may include:](#)

- physical monitoring **Due to the age or our children, internet use and use of digital technology is always supported by an adult.**
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- **responsibility for technical security resides with the Headteacher who may delegate activities to identified roles.**
- **all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Governor**
- all users will be provided with a username and secure password. Users are responsible for the security of their username and password, and must not allow other users to access the systems using their log on details.
- **all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.**

- the administrator passwords for school systems are kept in a secure place, via Lead IT
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, in the cloud,
- Lead IT are responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them. All such devices are encrypted and/or password protected.
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- the installation of programmes onto school devices can only be done by DCC or LEAD IT as appropriate or by system administrators (respectively Headteacher, Teacher, SBM).
- removable media is not permitted unless approved by the SLT/IT service provider (and MUST be encrypted school media)
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. The Headteacher, SBM and Teacher all have access to the server offsite, so data is secure.
- mobile device security and management procedures are in place. The school owns both ipods and ipads for education use, which utilise the school's wireless network. The devices then have access to the wider internet and other cloud based services. All users understand that the primary purpose of the use of mobile/personal devices in a school context is educational in line with other relevant school policies including but not limited to the safeguarding policy, behaviour policy, IT security and acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- guest users are provided with access to a guest network at the discretion of the Headteacher.

Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device ³	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Yes	n/a	No	No
Internet only	Yes	Yes	Yes	n/a	No	Yes
No network access	n/a	n/a	n/a	n/a	Yes	Guest access to a separate network

School owned/provided devices:

- the Headteacher, Teacher and SBM have allocated encrypted laptops and the Headteacher and Teacher have an allocated ipod/ ipad. All of the above are designated for use on and off site and have internet and network access on and off site.
- all other laptops and ipods/ pads are allocated for 'staff' use and are available for use by all staff on site as agreed by the Headteacher and teacher.
- all devices are for professional use only and have internet access subject to SNNS filtering. Laptops also have network access. Management of all staff devices is by LEAD IT in conjunction with the Headteacher.
- staff training, technical support and monitoring is provided by LEAD IT in conjunction with the teacher.

³ Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- all 'staff use' devices are stored on site at night (with the exception of Headteacher/teacher/ SBM devices allocated for home use).
- onsite all devices are subject at their respective level to SNNS school filtering provided by Lead IT (FTTC).
- images on mobile devices are for use during a child's time at nursery. All images are deleted after a child leaves nursery.

Personal devices:

- staff and visitors are only allowed to use personal devices at school during allocated break times of as agreed by the Headteacher and in areas not in use by the children.
- personal devices are stored in secure areas, away from the teaching areas in nursery in locked rooms or cupboards.
- where staff access work emails or Tapestry on personal devices, these devices and the sites are password protected, providing 2 factor authentication.
- staff do not access the schools network or broadband on their personal devices and are therefore not subject to SNNS filtering.
- it is staffs responsibility to ensure that they adhere to school policy. No technical support is available for personal devices. Advice may be sought from LEAD IT in conjunction with the teacher to ensure policy adherence.
- there is a clear policy covering the use of personal mobile devices on school premises for all users
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements (through the Code of Conduct for Visitors)

Social media

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.

School staff should ensure that:

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

- they do not engage in online discussion on personal matters relating to members of the school community.
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

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

- a process for approval by senior leaders (Headteacher, teacher and SBM)
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to private social media sites on personal devices at non teaching times and in non teaching spaces.

Monitoring of public social media

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

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

Digital and video images

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

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

- **the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.**
- **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In line with the age and understanding of the children staff ask permission to share children's images to Tapestry and nursery website, thus educating them about their right to give or withdraw permission to share.**
- **staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes. A list of those children whose images are not to be used on social media or the website is held by the SBM/Headteacher and Teacher.**
- in accordance with [guidance from the Information Commissioner's Office](#), parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images. **This information is shared with parents on entry, and reiterated by the Headteacher at public events.**

- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- photographs published on the website, or elsewhere that include pupils, will be selected carefully and will comply with Online Safety Policy
- **pupil's full names will not be used anywhere on a website or blog, particularly in association with photographs.**
- **written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. This is done in the admissions paperwork before children enter nursery. Parents can withdraw permission at any time. This information is shared with all staff.**
- **parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy**
- **images will be securely stored in line with the school retention policy**
- **students'/Pupils' full names will not be used anywhere on a website or blog. First names may be used if the permission of the parent is sought. Photographs of children will never be show with their name.**
- **student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.**

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters
- Tapestry

The school website is managed/hosted by Juniper Education. The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

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

The school **website** provides information about online safety e.g., publishing the schools Online Safety Policy and **IT Security and Acceptable Use Policy**; and we have a dedicated online safety page at the following link:

<https://www.southnormantonnurseryschool.co.uk/online-and-personal-safety/>

Data Protection

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

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest. **The Education Data Hub at DCC act as the DPO for South Normanton Nursery School.**
- has an 'information asset register' in place and knows exactly [what personal data is held](#), where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, **Governors**, volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice. **These can be found on the school website.**
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier

- IT system security is ensured and regularly checked by LEAD IT. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

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

- data will be encrypted, and password protected. (Headteacher, teacher and SBM laptops. All staff memory sticks)
- device will be password protected. (All devices including i-pods and i-pads)
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data

- **will not transfer any school personal data to personal devices. The Headteacher, Teacher and SBM all have remote access to the network.**
- **use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data**
- **transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.**

The Personal Data Advice and Guidance in the appendix (B2) provides more detailed information on the school’s responsibilities and on good practice.

Outcomes

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

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school’s online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice, and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe online safety self-review tool:

Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in September 2023. However, SWGfL cannot guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.

School Online Safety Policy

Template Appendices

Appendices

A1 - Responding to incidents of misuse – flow chart

A2 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A3 - Reporting Log

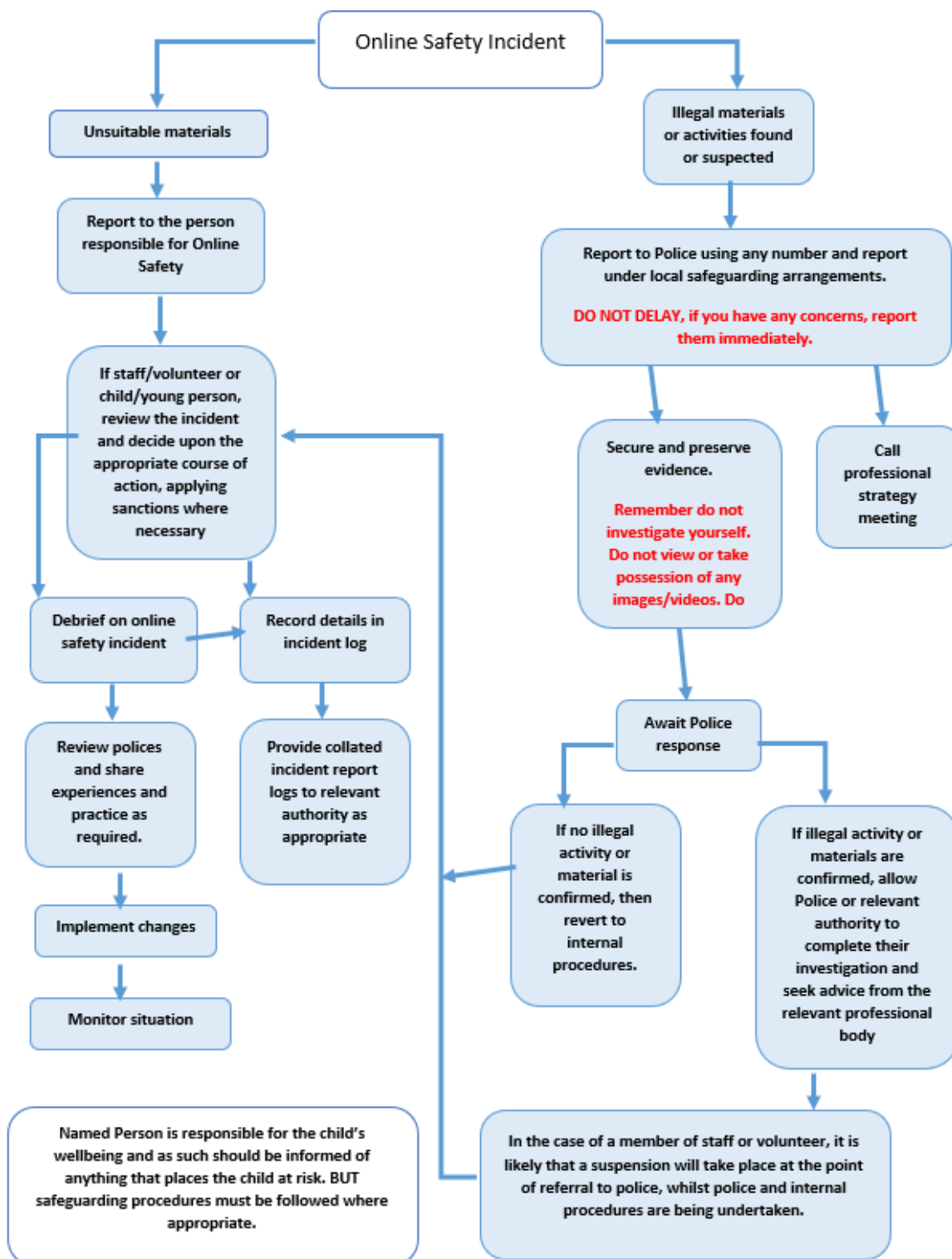
A4 - Training Needs Audit Log

Legislation

Links to other organisations and resources

Glossary of Terms

A1 Responding to incidents of misuse – flow chart



A2 Record of reviewing devices/internet sites (responding to incidents of misuse)

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 (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

A3 Reporting Log

Group:

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

B1 Training Needs Audit Log

Group:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Legislation

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

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

A useful summary of relevant legislation can be found at: [Report Harmful Content: Laws about harmful behaviours](#)

Computer Misuse Act 1990

This Act makes it an offence to:

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

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

Data Protection Act 1998

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

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.

- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

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.

Freedom of Information Act 2000

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

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience

or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

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

Regulation of Investigatory Powers Act 2000

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

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

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to

impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

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

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

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

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

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

The Education and Inspections Act 2006

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

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -

<http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carers to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

Serious Crime Act 2015

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

Criminal Justice and Courts Act 2015

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

For further guidance or support please contact the [Revenge Porn Helpline](#)

Links to other organisations or documents

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

UK Safer Internet Centre

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

CEOP

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

Others

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

Tools for Schools / other organisations

Online Safety BOOST – <https://boost.swgfl.org.uk/>
360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - <http://testfiltering.com/>
UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>
[SWGfL 360 Groups – online safety self review tool for organisations working with children](#)
[SWGfL 360 Early Years – online safety self review tool for early years organisations](#)

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harassment](#)

[UKSIC – Sexting Resources](#)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

Digizen – [Social Networking](#)

UKSIC - [Safety Features on Social Networks](#)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

Curriculum

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/

Insafe - [Education Resources](#)

Data Protection

[360data - free questionnaire and data protection self review tool](#)

[ICO Guides for Organisations](#)

[IRMS - Records Management Toolkit for Schools](#)

[ICO Guidance on taking photos in schools](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[Childnet – School Pack for Online Safety Awareness](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

Somerset - [Questions for Technical Support](#)

SWGfL - [Cyber Security in Schools](#).

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[SWGfL – Online Safety Guidance for Parents & Carers](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

Childnet – [Trust Me](#)

Research

[Ofcom –Media Literacy Research](#)

Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)

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.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
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
MAT	Multi Academy Trust
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 Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
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
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in September 2023. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.