Sandy Lane Nursery and Forest School
"Nurturing curiosity and inspiring imagination"



2026-27
Online Safety Policy

DOCUMENT STATUS

Produced By	Version	Date	Action
Sandy Lane Nursery and Forest School *With acknowledgement to Aspiring Foundations Federated Nursery Schools*	1	07.02.23	Approved by Resources Committee
	2	30.01.24	Annual review by Resources Committee
		04.02.25	Annual review by Resources Committee
	3	07.10.25	Approved by Resources Committee
	4	20.10.26	Approved by Resources Committee

Legislation

- General Data Protection Regulation 2018
- UK Data Protection Act 2018
- Human Rights Act 1998
- Computer Misuse Act 1990, Computer Misuse Act 2011 and Computer Misuse (Amendment) Act 2022
- Keeping Children Safe in Education 2026
- Working Together to Safeguard Children 2026
- Prevent Duty Guidance 2023 (issued under s29 of the *Counter-Terrorism and Security Act 2015)*
- The Prevent Duty - Departmental advice for schools and childcare providers 2024
- Guidance for safer working practice for adults who work with children and young people in education settings 2022
- Obscene Publications Act 1959 and 1964

Approval

Governing body free to delegate to a committee of the governing body, an individual governor or the headteacher

Review Frequency

Annually

Amendments

v2

- Legislation updated
- s5, *Ensuring the Safe and Appropriate Use of Mobiles Phones and Electronic Devices* (p5) – includes reference to smart phones; and permission for making emergency calls during working hours
- s5, *Use of Mobile Phones and Electronic Devices for Volunteers and Visitors* (p5) – includes reference to smart phones
- s9, *Responding to Incidents of Misuse* – includes reference to updated Computer Misuse (Amendment) Act 2022 (see table on p8)
- s16, *Local/National Lockdown* (p12) – parents to check any links to websites before sharing with children

v3

- Additional section on AI (Artificial Intelligence) (s6)
- Contents re-ordered

v4

- Legislation updated

	CONTENTS	PAGE No
1	Responsibilities	4
2	Prevent Duty	4
3	Photographs and Videos	5
4	Mobile Phones and Other Devices	5
5	Emails	7
6	Artificial Intelligence (AI)	7
7	Security and Passwords	7
8	Data Storage	8
9	Unsuitable/Inappropriate Activities	8
10	Responding to Incidents of Misuse	8
11	Illegal Incidents	11
12	Other Incidents	12
13	School Actions and Sanctions	13
14	Social Networking	14
15	Online safety Education	14
16	Parents and the Wider Community	14
17	Local/National Lockdown	14
18	Monitoring and Reporting	15
19	Acceptable Use Policy Guidance for School and Governors	15
Appendix 1	Record of Reviewing Devices/Internet Sites	17
Appendix 2	Reporting Log	19

Sandy Lane Nursery and Forest School Online Safety Policy

This policy should be viewed alongside the following school policies which have relevance to safeguarding:

- Safeguarding and Child Protection
- Whistleblowing
- Staff Code of Conduct
- Allegations Against Adults
- Data Protection
- Data Security (Data Breaches)
- Low Level Concerns
- Social Media

1 Responsibilities

The member of staff responsible for online safety is - **Kirsten Matthews** as Safeguarding Lead. Kirsten is responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote online safety within the school community. She may also oversee the delivery of workshops for parents.

Internet use and Acceptable Use Policies (AUPs) - all members of the school community should agree to an Acceptable Use Policy that is appropriate to their role.

The children at nursery school are deemed to be too young to complete an AUP. AUPs will be reviewed annually. All AUPs will be stored centrally in case of breaches of the online safety policy.

2 The Prevent Duty

The Prevent Duty is the duty in the *Counter-Terrorism and Security Act 2015* on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism. The general risks affecting children and young people may vary from area to area and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context. They should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. For Sandy Lane Nursery and Forest School, this is provided via a Warrington Borough Council service level agreement. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff need

to be aware of the risks posed by the online activity of extremist and terrorist groups. The Prevent Duty means that all staff have a duty to be vigilant and, where necessary, report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a school's monitoring and filtering systems to be fit for purpose. For Sandy Lane Nursery and Forest School, these are provided via a Warrington Borough Council service level agreement.

3 Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used. If photos/videos are to be used online, then names of pupils should not be linked to them. Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise. Staff should always use a school camera to capture images and should not use their personal devices.

Children are deemed to be too young to be at risk to any exploitation arising from 'upskirting'. Where children use mobile devices to take photographs around the provision, they are always supervised by an adult. Mobile devices are not allowed into the bathroom areas. Mobile devices are only used online by children in the presence of an adult. They are also covered by web filtering. Photos taken by the school are subject to the *UK Data Protection Act 2018*.

Photos and videos taken by parents/carers - parents and carers visiting school are asked to leave their mobile phones securely in the school office. They are not permitted to take photos/videos of children in school or on school visits. Staff will use school devices to take photos/videos of these events which will be posted for parents and carers on Tapestry. Prior to being given access to Tapestry families give consent that images will not be shared on social networking sites or with other adults via the Tapestry consent as part of their new intake pack. Reminders are given to parents and carers at the start of any event they attend by school staff

4 Mobile Phones and Other Devices

Sandy Lane Nursery and Forest School recognises that there may be occasions when staff need to have access to mobile phones during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings. The concerns are mainly based around these issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones and Electronic Devices

- Sandy Lane Nursery and Forest School allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device
- The use of mobile phones and similar devices whilst on duty within the childcare environment is strictly forbidden
- Staff must ensure that personal mobile phones or other electronic devices are not carried about their person during working hours and MUST be stored in their personal lockers or, in the case of supply staff, in the locker allocated to them. In the case of smart watches, notifications must be switched off during working hours
- Personal mobile phones must be kept in lockers provided during working hours, although can be used during lunch breaks in the staff room, meeting room or main office
- Using a mobile phone to take pictures or video clips of children is not allowed
- Where trips are taken outside of the school, staff MUST NOT use a personal mobile. The school provides a school mobile for this purpose which the trip leader must make sure is fully charged and switched on for the duration of the trip. If staff fail to follow this guidance, disciplinary action will be taken in accordance with the school's Staff Code of Conduct
- If staff need to make an emergency call, they must do so with the permission of SLT, either in the main or headteacher's office or the staffroom. Staff must ensure that there is no inappropriate or illegal content on the device

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school. Children should not use mobile phones within the school grounds and should not bring in a mobile to school at any time.

Use of Mobile Phones and Electronic Devices for Volunteers and Visitors

When visiting school, volunteers and visitors are given information informing them that they are not permitted to use mobile phones on the premises. Parents, carers and visitors based in classrooms are required, on entry to the building, to leave devices securely in the school office and collect them on exit. In the case of smart watches, all visitors and volunteers will be asked to turn off notifications until they have signed out. Other professionals visiting to observe children, eg, an educational psychologist, will be required to leave their personal mobile in the office they have been assigned to work in, along with other personal items. Any such adult wishing to make or take an emergency call may use either the main or head teacher's office or the staffroom. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the head teacher's permission. Important contact details of the children are kept in the office. In case of an emergency, contact with a parent is made via the school office. This includes any contact that may need to be made with a parent whilst children are on an educational visit.

We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the pre-school environment; sometimes this will be when children

are engrossed in an activity, either on their own or with their peers. Children are encouraged to use the camera to take photos of their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All staff at the school understand the difference between appropriate and inappropriate sharing of images. All images are kept securely in compliance with the *UK Data Protection Act 2018*.

If a member of staff suspects that a mobile phone has been misused within the school, then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to the senior leadership team (SLT) which will deal with the matter in line with normal school procedures.

5 Use of E-Mails

The e-mail system should only be used for school related matters. Staff are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

6 Artificial Intelligence (AI)

At Sandy Lane Nursery and Forest School, we are aware of the potential risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

Staff will always:

- use generative AI tools ethically and responsibly
- ensure that AI solutions are approved, secure and safe for users and protect users' data
- remember the principles set out in our school's equality policy when using generative AI tools (available on the school website)
- consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- fact and sense-check the output before relying on it

Staff and governors will not:

- generate content to impersonate, bully or harass another person
- generate explicit or offensive content
- input offensive, discriminatory or inappropriate content as a prompt

Please see Use of Artificial Intelligence (AI) Policy which outlines the established guidelines for the ethical, secure and responsible use of AI technologies across our whole school community.

7 Security and Passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image

to remain on the screen and also allow a PC to be 'locked'). All users should be aware that the ICT system is filtered and monitored.

8 Data Storage

The school uses a 'cloud' based system so no USB pens, encrypted or otherwise, are to be used in school.

9 Dealing with Unsuitable/Inappropriate Activities

Some internet activity, for example accessing child abuse images or distributing racist material, is illegal and would obviously be banned from school and all other technical systems. Other activities, for example cyber-bullying, would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

10 Responding to Incidents of Misuse

This guidance is intended for use when staff 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 involve illegal or inappropriate activities. Sandy Lane Nursery and Forest School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

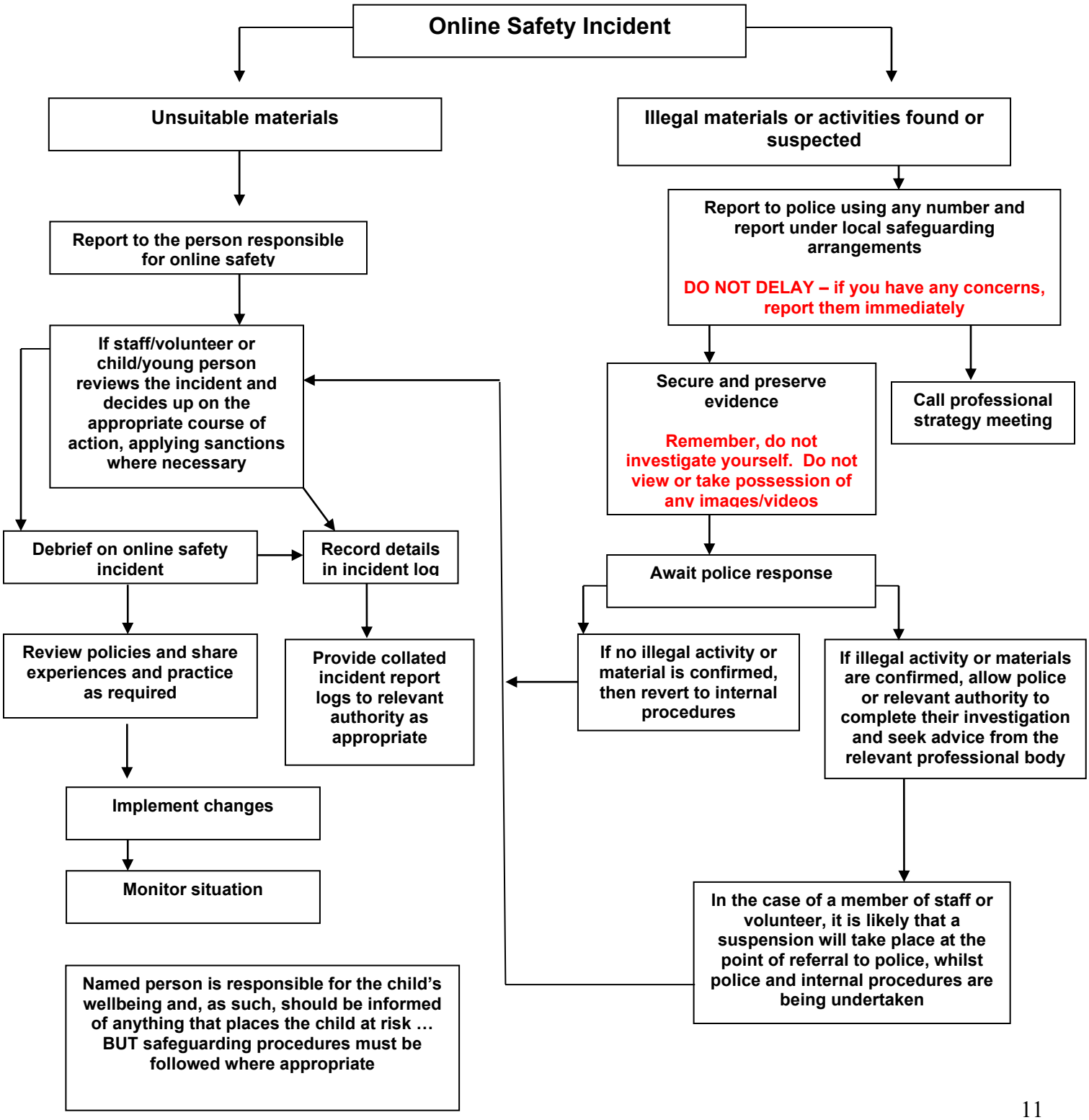
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – the making, production or distribution of indecent images of children, contrary to the *Protection of Children Act 1978* NB – schools should refer to guidance about dealing with self-generated images/sexting: UKSIC responding to and managing sexting incidents (https://saferinternet.org.uk/blog/responding-to-and-managing-sexting-incidents-updated-advice-for-schools); and UKCIS sexting in schools and colleges (https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)					X

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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 *Public Order Act 1986*					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation), contrary to the *Criminal Justice and Immigration Act 2008*					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 school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the *Computer Misuse Act 1990*: • 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 (eg, 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) Note that the *Computer Misuse (Amendment) Act 2022* amends the *Computer Misuse Act 2011* by*:* • *enhancing the provisions on unauthorised access to information or data;* • *prohibiting unlawful sharing of any information relating to a child;* • *prohibiting hate speech, the sending or sharing of malicious or unsolicited information;* • *regulating the use of social media; and for related matters.* NB – we take the view these types of offence would be classed as cyber-crime						X X X X

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
and a deliberate attack on the security of the school and, therefore, we would seek further support from the local authority and the police. Serious or repeat offences would be reported to the police					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Revealing or publicising confidential or proprietary information (eg, financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinder others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
Online gaming (educational)				X	
Online gaming (non-educational)				X	
Online gambling				X	
Online shopping/commerce		X			
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting, eg, Youtube		X			

11 Illegal Incidents

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



12 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff 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 *responding to incidents of misuse* form – see appendix 1 (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
    - ❖ 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
    - ❖ Adult material which potentially breaches the *Obscene Publications Act 1959*
    - ❖ Criminally racist material
    - ❖ Promotion of terrorism or extremism
    - ❖ Offences under the *Computer Misuse Act* (see User Actions chart above)
    - ❖ The criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police, and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes

13 School Actions and Sanctions

It is more likely that Sandy Lane Nursery and Forest 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:

	Staff Incidents	**Refer to line manager**	**Refer to headteacher**	**Refer to local authority**	**Refer to police**	**Refer to IT for action on filtering**	**Warning**	**Suspension**	**Disciplinary action**
1	Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		X	X	X				
2	Inappropriate personal use of internet/social media/personal email		X				X		X
3	Unauthorised downloading or uploading of files		X			X	X		X
4	Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X	X		X
5	Careless use of personal data, eg, holding or transferring data in an insecure manner		X	X			X		
6	Deliberate actions to breach data protection or network security rules		X	X					X
7	Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					X
8	Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					X
9	Using personal email/social networking/instant messaging/text messaging to carry out digital communications with children		X						X
10	Actions which could compromise the staff member's professional standing		X				X		
11	Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X		X
12	Using proxy sites or other means to subvert the school's filtering system		X			X	X		X
13	Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X		
14	Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
15	Breaching copyright or licensing regulations		X	X		X			X
16	Continued infringements of the above, following previous warnings or sanctions		X	X					X

14 Social Networking

Pupils are not permitted to use social networking sites within school.

15 Online safety Education

Pupils
Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum via the *KidSafeUK* programme. A series of awareness-raising activities is also shared with families via Tapestry as part of the *You Think U Know* programme. In addition, where staff post links to websites, parents and carers are reminded to review the link prior to sharing with children.

Staff

a) A planned programme of formal online safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent Duty.
b) Online safety training is an integral part of child protection/safeguarding training and vice versa.
c) All staff have an up-to-date awareness of online safety matters, the current school online safety policy and practices and child protection/safeguarding procedures.
d) All new staff receive online safety training as part of their safeguarding induction programme, ensuring that they fully understand the school online safety policy and acceptable use policy.
e) The culture of the school ensures that staff support each other in sharing knowledge and good practice about online safety.
f) The school takes every opportunity to research and understand good practice that is taking place in other schools.
g) Governors are offered the opportunity to undertake training.
h) Any staff member who is concerned about online safety or wants further advice about applications (apps)/online bullying or harassment can also access free advice about the professional online safety help line 0344 381 4772; helpline@saferinternet.org.uk.

16 Parents and the Wider Community

Parents are also supported to start to develop good habits about online safety at home and to learn about family safety planning. This is offered as part of the *You Think U Know* series of activities and the *KidSafeUK* programme delivered to children and shared with families.

17 Support for Children who are attending Sandy Lane Nursery and Forest School during a Local/National Lockdown or prolonged school closure

Due to the practical nature of learning for young children, it is unlikely that school staff will ever teach online, however if staff were to need to contact children online, then the following will be considered:

- No 1-1 discussions – group learning only
- Where possible, any online support (eg, a story session) would be pre-recorded, will take place in an appropriate room and staff will ensure that they are wearing appropriate attire

- Practical fun ideas will be posted to parents daily via Tapestry to guide and support them in working with their child at home. Parents are reminded to check any links to websites shared by school prior to showing their children. Parents are also encouraged to add to their child's online portfolio by sending in photos/observations of their children engaging in activities at home. These are all sent in via:
    - ❖ Tapestry and stored in the online journal and their child's folder only
    - ❖ Staff will only use online platforms that have been agreed with the headteacher
    - ❖ Staff should ensure that the headteacher/deputy headteacher is aware of the online support being given, along with the date and time that it is being shared

18 Monitoring and Reporting

a) The school network provides a level of filtering and monitoring that supports safeguarding.
b) The impact of the online safety policy and practice is monitored through the review/audit of online safety incident logs (see appendix 2), behaviour/bullying logs, surveys of staff, students/pupils, parents/carers.
c) The records are reviewed/audited and reported to:
    - ❖ the school's senior leaders
    - ❖ Governors
    - ❖ Warrington local authority (where necessary)
    - ❖ Warrington and Halton Safeguarding Children Board
d) The school action plan indicates any planned action based on the above.

19 AUP (Acceptable Use Policy) Guidance Notes for School and Governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones, etc) is used to support learning without creating unnecessary risk to users.

The governors will ensure that:

- Learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- Learners are made aware of risks and processes for safe digital use
- All adults and learners have received the appropriate acceptable use policies and any required training
- The school has appointed a staff member responsible for online safety, ie, Kirsten Matthews as DSL; and our link governor is our safeguarding governor
- An online safety policy has been written by the school
- The online safety policy and its implementation will be reviewed annually
- The school internet access is designed for educational use and will include appropriate filtering and monitoring
- Copyright law is not breached
- Learners are taught to evaluate digital materials appropriately
- Parents are aware of the AUP and give consent regarding arrangements for photos and videos shared on Tapestry
- Parents will be informed that all technology usage may be subject to monitoring, including

URLs (Uniform Resource Locators, ie, the names of given resources on the web) and text

- The school will take all reasonable precautions to ensure that users access only age-appropriate material
- The school will audit use of technology to establish if the online safety policy is adequate and appropriately implemented
- Methods to identify, assess and minimise risks will be reviewed annually
- Complaints of internet misuse will be dealt with by a senior member of staff

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 websites)

……

Website(s) address/device	**Reason for concern**
Conclusion and action proposed or taken	

Reporting Log

Reporting Log

Group: ……..

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