Rowley View Nursery

Online Safety Policy

Signed	**Chair of Governors**
Date	**December 2022**

Development / Monitoring / Review of this Policy

This Online Safety Policy has been developed by: -

- Head teacher and Senior Leadership Team
- Governors

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by Governing Body on: -	December 2022
The implementation of this Online Safety policy will be monitored by the:	Julia Julian (Head teacher)
Monitoring will take place at regular intervals:	Annually
The Governing Body 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:	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	November 2023
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Officer, MASH, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the nursery school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of nursery school digital technology systems, both in and out of the nursery school.

The Education and Inspections Act 2006 empowers Head teacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the nursery school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the nursery school, but is linked to membership of the nursery school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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.

Rowley view Nursery identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the nursery school.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. Governors will also receive regular training about online safety in line with their safeguarding training on an annual basis. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

Head teacher and Senior Leaders

- The Head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer.
- The Head teacher and Rachel Dudley, another member of the Senior Leadership Team, should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Head teacher/ Senior Leaders are responsible for ensuring that the Online Safety Officer / Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher/ Senior Leaders 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Online Safety Lead – Julia Julian / Rachel Dudley

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff

The Technical Staff is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the nursery school meets required online safety technical requirements and any Local Authority / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that 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

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current nursery school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem by emailing their concern to the Head teacher/DSL / Online Safety co-ordinator/ for action / sanction
- all digital communications with students / pupils / parents / carers should be 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, where appropriate to our nursery school
- students/parents understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons internet use should be pre-planned students / pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is reported immediately.

Designated Safeguarding Lead – Julia Julian

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Pupils:

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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The nursery school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the nursery school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

Practice

Our setting has clear and effective procedures in place to manage online safety incidents for all users.

The use of technology is managed at the setting through:

- Supervision of children when online

- When internet is used, we manage access to online content through appropriate filtering **(see section below)**
- Regular review of practice

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

Staff are aware of how to keep children safe.

Filtering and Monitoring

The school uses Internet filtering and firewall – 'Fortigate' Filter. The filtering system is designed to prevent access to inappropriate content, it does not unreasonably restrict the online activities at Rowley view Nursery School. Staff know they should check websites prior to a session when they are being used with children too to prevent viewing inappropriate content.

The network is monitored by Smoothwall monitor a service school buys into from Walsall Online monitoring service. This software is installed on all networked machines and monitors both viewed and typed captures. Any incidents that are flagged mean the DSL receives an online incident report to investigate and action. This includes all levels of incidents from Level 1 – 5. 5 being the most serious.

Security

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

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

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

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

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

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

- Blocked access to illegal content on our systems through filtering and **regularly** test its effectiveness – we use – http://testfiltering.com/
- Ensured staff/volunteers only have access to appropriate agreed content on our systems through appropriate access and filtering
- Ensured appropriate access to online content used by children through supervision, filtering and the use of child friendly search engines e.g. SWGfL Swiggle
- Effective monitoring in place to alert us to any illegal access or misuse of our systems

Policy Statements

Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. 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 should be provided as part of PHSE / other lessons/stories and should be regularly revisited
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside nursery school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

Education – Parents / Carers

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

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education and Training – Staff / Volunteers

It is essential that all staff 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 training will be made available to staff. This will be regularly annually and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the nursery school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL / 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 meetings.
- The Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in nursery school training / information sessions for staff or parents

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the GDPR legislation). To

respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or social media, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media

Data Protection – related to GDPR

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school / academy must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out, when appropriate.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.

- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- Have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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: -

- 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 and secure password protected devices.
- Expected to change their school passwords at least once a term.

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

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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages: -

Communication Technologies	Staff & other adults			Parent and carers				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the nursery school				x				x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices e.g. tablets, gaming devices				x				x
Use of personal email addresses in nursery school, or on nursery school network				x				x
Use of nursery school email for personal emails				x				x
Use of messaging apps			x					x
Use of social media			x					x

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

- The official nursery school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the nursery school email service to communicate with others when in school, or on nursery school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the nursery 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.
- Any digital communication between staff and parents / carers (email, social media, chat, etc.) must be professional in tone and content.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the nursery school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

The nursery school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through: -

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Nursery school staff should ensure that: -

- No reference should be made in social media to pupils, parents / carers or nursery 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

On the official nursery school social media account (Facebook): -

- All posts are approved by senior leaders
- Four senior members of staff have been appointed as administrators of the account and are responsible for monitoring it. They have notifications set up for the account to ensure that they are vigilant with monitoring
- Parents are notified during induction and within the parent handbook of the code of behavior for our Facebook page. The page permission is set up so they cannot add their own personal posts to the page
- They are informed that legal advice / action may be taken for any posts that may bring the school into disrepute on their own personal Facebook pages and the system for reporting any concern.
- Parents can privately message the school Facebook page or phone the school within office hours to report any concerns or suspected misuse. Staff can message the school WhatsApp page or phone a member of the senior leadership team directly, to report any concern or suspected misuse.

Personal Use: -

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the nursery school or impacts

on the school, it must be made clear that the member of staff is not communicating on behalf of the nursery 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 nursery school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from nursery school and all other technical systems. Other activities e.g. online-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.

The nursery school believes that the activities referred to in the following section would be inappropriate in a nursery school context and that users, as defined below, should not engage in these activities in / or outside the nursery school when using nursery school equipment or systems.

The nursery 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					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the nursery school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			x			
On-line gaming (non-educational)					x	

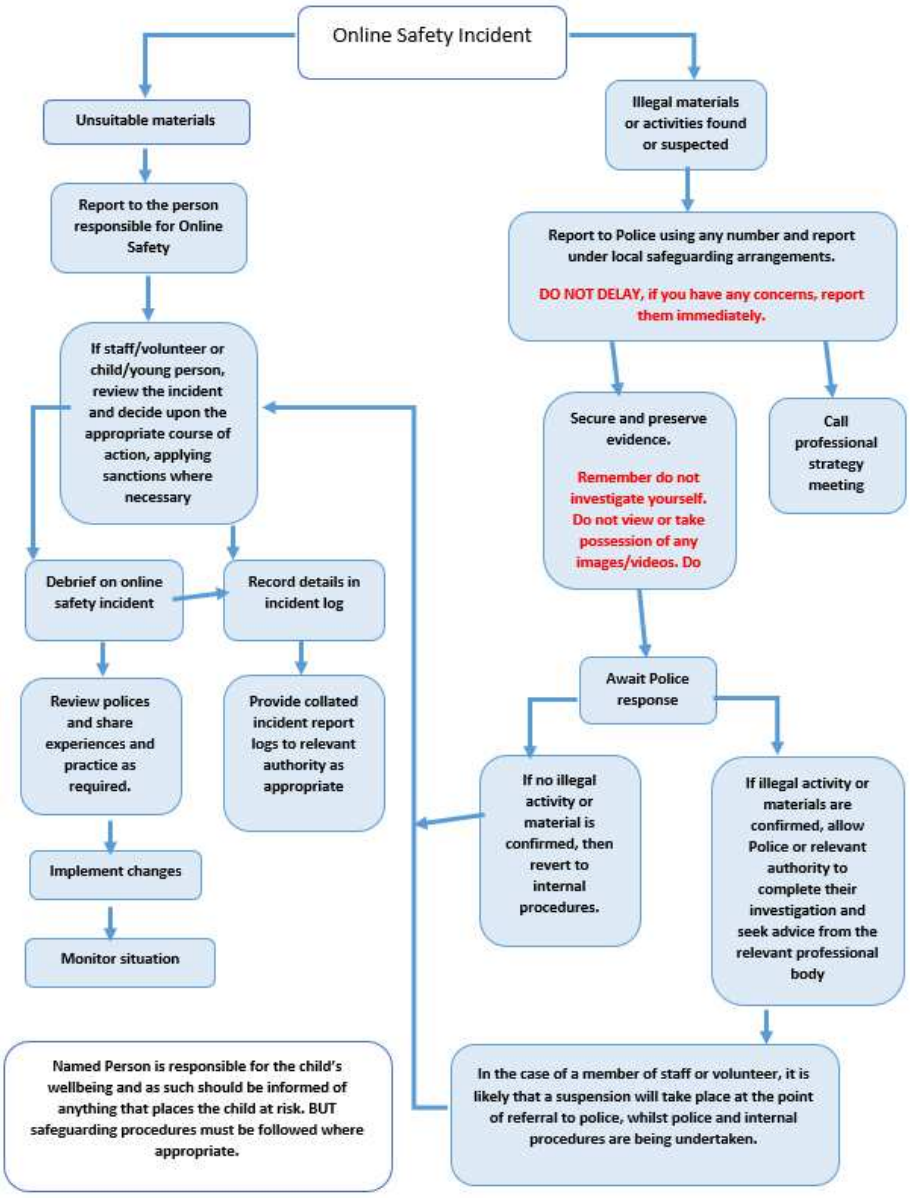
On-line gambling				x	
On-line shopping / commerce		x			
File sharing	x				
Use of social media		x	x		
Use of messaging apps			x		
Use of video broadcasting e.g. You tube		x			

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 (see “User Actions” above)

Illegal Incidents

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



Other Incidents

It is hoped that all members of the nursery school community will be responsible users of digital technologies, who understand and follow nursery 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 young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following: -
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - 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
    - criminally racist material
    - promotion of terrorism or extremism
    - other 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 nursery 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.

Nursery school actions and Sanctions

It is more likely that the nursery 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: -

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	x	x	x	x	X	x	x	x
Inappropriate personal use of the internet / social media / personal email	x	x	x	x	X	x	x	x
Unauthorised downloading or uploading of files	x	x	x	x	X	x	x	x
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x	x	x	X	x	x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x	x	X	x	x	x
Deliberate actions to breach data protection or network security rules	x	x	x	x	X	x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x	x	X	x	x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x	X	x	x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	x	x	x	x	X	x	x	x
Actions which could compromise the staff member's professional standing	x	x	x	x	X	x	x	x

Actions which could bring the nursery school into disrepute or breach the integrity of the ethos of the nursery school	x	x	x	x	X	x	x	x
Using proxy sites or other means to subvert the school's filtering system	x	x	x	x	X	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x	X	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	X	x	x	x
Breaching copyright or licensing regulations	x	x	x	x	X	x	x	x
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x	X	x	x	x

Staff Misuse

Any complaint about staff misuse will be referred to the Head Teacher, in accordance with the allegations policy.

Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

Appendices

Parent / Carer Acceptable Use Agreement – Completion not currently required due to the children having access to only one PC with no internet access

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

- This form is printed for parents and completed forms will be accessed by the administrative office staff.
- The form will be stored in a locked office cabinet for the length of the child's education in school.
- It will then be placed in the secure confidential waste bin to be destroyed.

Signed: - _____

Date: - _____

Use of Digital / Video Images – school proforma currently in use

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publically shared by any means, only your child's first name/initials will be used.

The school will comply with the Data Protection Act and request parent / carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

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

- This form is printed for parents and completed forms will be accessed by the administrative office staff.
- The form will be stored in a locked office cabinet for the length of the child's education in school.
- It will then be placed in the secure confidential waste bin to be destroyed.
- The images may be published on the school Facebook page, the nursery school website or the parent handbook.
- The images will be accessed by administrative staff and senior leaders. The hard copy will be deleted after being uploaded/ added to the platform.
- Images will be changed annually and will be permanently deleted from the school system.
- A parent /carer can make a request to have an image deleted by contacting the school office in writing via email or post.

Digital / Video Images Permission Form – School proforma currently in use

Parent / Carers Name: - _____ Pupil Name: - _____

As the parent / carer of the above pupil, I agree to the school taking digital / video images of my child / children. I agree to these images being used: -	Yes / No
• to support learning activities.	Yes / No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
Insert statements here that explicitly detail where images are published by the nursery school	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Date: .....

Staff Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety: -

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

- I will set strong passwords (a strong password is one which uses a combination of letters, numbers and other permitted signs)
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school Computing systems: -

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Rowley View Nursery School: -

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices, smart watches etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use: -

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of Rowley View Nursery School: -

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name: - _____

Signed: - _____

Date: - _____

Pupil Acceptable Use Policy

