Templemoor Infant and Nursery School

Online Safety Policy

Policy Adopted	7th October 2017
Committee	Resources and Safety and Full Governing Body
Last Reviewed	2nd February 2022
Next Review Date	February 2023

Due to the ever changing nature of digital technologies, this Online SafetyPolicy will be reviewed at least annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. This Policy has been written using guidance from South West Grid for Learning (SWGL) and 360 Degree Safe.

Templemoor Infant and Nursery School
Online Safety Policy

Scope of the Policy

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

Roles and Responsibilities

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

The Governing Body

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 Resources and Safety Committee receiving regular information about online safety incidents and monitoring reports.

The Governor responsible for online safety is Mrs Judith Davenport. The role of the Online Safety Governor includes:

- regular meetings with the Online Safety Lead, Mr Stuart Hodgson.
- regular monitoring of online safety incident logs.
- regular monitoring of filtering logs.
- reporting to relevant Governors.

The Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of all members of the school community.

The Headteacher, Deputy Headteacher and Early Years Lead must be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – 'Responding to incidents of misuse').

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead/ Designated Safeguarding Lead

The Online Safety Lead is the Designated Safeguarding Lead, Mr Stuart Hodgson. The Online Safety Lead:

- leads on online safety issues.
- 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 external technicians (One Education).
- receives reports of online safety incidents via CPOMS and regularly reviews the log of incidents to inform future online safety developments.
- meets regularly with the Online Safety Governor to discuss current issues and to review incident logs and filtering logs.
- reports to the Resources and Safety committee and to the Full Governing Body.
- Is aware of the potential for serious child protection/safeguarding issues arising 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

Network Manager and Technical Support

Templemoor Infant and Nursery School has a managed ICT service provided by One Education. Technical Support is provided by One Education.

Those with technical responsibilities are responsible for ensuring:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the required online safety technical requirements and any Local Authority/other relevant body Online Safety Policy/Guidance that may apply.
- Users may only access the networks and devices through properly enforced password protection, in which passwords are regularly changed.
- 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.
- The use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Online Safety Lead for investigation/action/sanction.
- Filtering and monitoring software/systems are implemented and updated.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- They have read, understood and signed the Staff Acceptable Use Agreement (AUA).
- They report any suspected misuse or problem to the Headteacher for investigation/action/sanction.
- All digital communications with children/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.
- Children understand and follow the Online Safety and acceptable use agreements.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities and implement current policies about these devices.
- In lessons where internet use is pre-planned children 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

Pupils

- Agree to follow the 'Acceptable Use Agreement for Children.'
- Take responsibility for learning about the benefits and risks of using the internet and other technologies at school and at home.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- Discuss online safety issues with family and friends in an open and honest way.

Parents and 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 school will take every opportunity to help parents understand these issues through parents' information evenings, newsletters, letters, the school website and information about national/local online safety campaigns/literature.

Parents/carers are expected to:

- Help and support the school in promoting good online safety practice.
- Read, understand and promote the school's 'Acceptable Use Agreement for Children' with their children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss online safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology at home.
- Model safe and responsible behaviour in their own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.

Parents and carers will be encouraged to support the school to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to the parents' sections of the website/Learning Platforms and on-line pupil records

their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User Acceptable User Agreement before being provided with access to the school system. (A community users acceptable use agreement can be found in the appendices.

Education – Children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children 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 need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In planning our online safety curriculum, the school has used:

- DfE 'Teaching Online Safety in Schools'.
- The 'Education for a Connected World Framework'.

We believe that the key to developing safe and responsible behaviour online, not only for children but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our children' lives not just in school but outside as well, and we believe we have a duty to help prepare our children to benefit safely from the opportunities the Internet brings.

- We will provide specific half-termly online safety related lessons in every year group as part of the Computing and PHSE/RSE curriculum. This will be regularly revisited.
- We will celebrate and promote online safety through assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant online safety messages with children routinely, in an age-appropriate way, wherever suitable opportunities arise during all lessons.
- We will remind children about their responsibilities through the school's 'Acceptable Use Agreement for Children,' which will be sent home with children for them to read and to share with parents.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Children should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- It is best practice that children 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.

Education – Parents and Carers

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Arrange online safety talks and training, linking with Moorlands Junior School when possible.
- Include useful links and advice on online safety regularly in newsletters and on our school website.
- Provide information and awareness to parents and carers through high profile events and campaigns e.g. Safer Internet Day.
- Include a page on online safety on the school website with links to relevant online safety websites and publications.
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers.

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- The school website will provide online safety information for the wider community.

Education & 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 online safety training will be made available to staff.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Designated Safeguarding Lead will receive regular updates through attendance at external training events/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 Designated Safeguarding Lead will provide advice/guidance/training to individuals as required.

Training – 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 a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisations.
- Participation in school training/information sessions for staff or parents.
- Online training.

Technical – Infrastructure/ equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible through the following:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The 'master/administrator' passwords for the school, used by the Network Manager must also be available to the Headteacher and School Business Manager and kept in a secure place.

- The One Education Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. There is a clear process in place to deal with requests for filtering changes (see appendix for more details).
- Internet filtering/monitoring must ensure that children are safe from terrorist and extremist material when accessing the internet.
- An appropriate system is in place for users to report any actual/potential technical incidents/security breaches to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. 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 devices are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of 'guests' (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- All users will agree to an Acceptable Use Agreement (AUA) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using the school ICT systems, and that such activity will be monitored and checked.
- All children are logged on as children on the school network, only allowing them access to certain areas. Internet access will be supervised by a member of staff.
- Members of staff will access their internet through their own individual log on.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.
- The school uses a filtered internet service, **'Sophos XG Firewall'** provided by One Education, which is CIPA compliant.
- The school will regularly audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate. We will regularly review our Internet access.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils 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:

- When using digital images, staff should inform and educate children 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.
- Written permission from parents or carers will be obtained before photographs of pupils are

published on the school website/social media/local press and in school newsletters.

- 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 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 pupils in the digital/video images.
- Staff 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 must 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, particularly in association with photographs.
- Staff will follow the school Social Media Policy on the use of photographs, videos, mobile phones and social networking sites.

Data Protection

The school ensures that:

- It has a Data Protection Policy in place and that this is reviewed regularly.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and has a named Data Protection Officer (DPO).
- The Data Protection Officer (DPO) has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it.
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded.
- It will hold only 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. The school has a 'Retention Policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. Personal data held must be accurate and up to date where this is necessary for the purpose it is processed for.
- It provides staff, parents, volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- Procedures are in place to deal with the individual rights of the data subject.
- IT system security is regularly checked.

- It has undertaken appropriate due diligence and has data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law.
- It has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data protection training at induction and appropriate refresher training thereafter.

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

- device must be password protected.
- device must be protected by up-to-date virus and malware checking software.
- data must 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:

- ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- access personal data sources and records 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

Communications

Using e-mail

Staff have their own school e-mail accounts which they use at home and at work. All staff can also be contacted through the school email address admin@templemoor.trafford.sch.uk

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications can be monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

Users must immediately report, to the nominated person – 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.

Using mobile phones

- Staff will not use personal mobile phones in any situation around children in the school or classroom.
- Staff will not use their personal mobile phone in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

- Staff can, however, use personal mobile phones on school trips to keep in touch with school and for dealing with any emergencies.

Using new technologies

- As a school we will keep informed of new technologies and consider both the benefits for learning and teaching and also the risks from an online safety point of view.
- We will regularly amend the Online Safety Policy to reflect any new technology that we use, or to reflect the use of new technology by children which may cause an online safety risk.

The school website

- The school website will not include the personal details, including individual e-mail addresses or full names of children.
- All content included on the school website will be approved by the Headteacher before publication.
- Permission from parents will be sought before any photographs of children are used on the school website.
- Staff and children should not post school-related content on any other external website without seeking permission first.

Dealing with unsuitable/inappropriate activities

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

The 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	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978. N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and					X

communicate or pass on, material, remarks, proposals or comments that contain or relate to:	managing sexting incidents and UKCIS – Sexting in schools and colleges					
	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, using 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 using computers/devices • Using penetration testing equipment (without relevant permission) N.B. School 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. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	

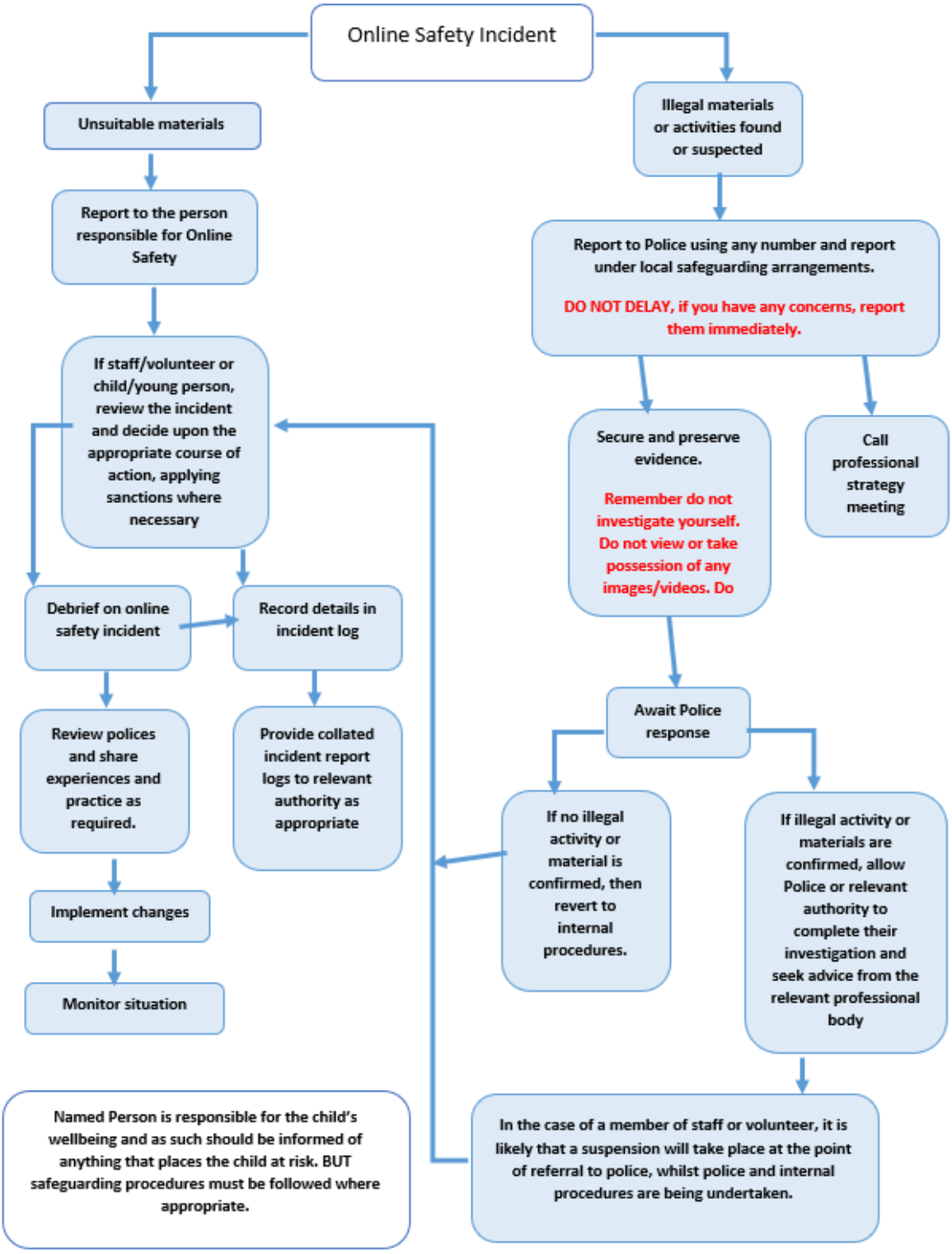
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce		X			
File sharing		X			
Use of social media			X		
Use of messaging apps		X			
Use of video broadcasting e.g., Youtube		X			

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.

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 and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

In the event of an online safety incident, ensure that:

- Children are directed away from any harm (e.g., viewing of unsuitable material)
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern to One Education, who can be contacted on **0844 967 1113**. 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
    - 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
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- Isolate the computer equipment 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 for evidence and reference purposes.

Inappropriate Use by Staff or Adults

If a member of staff is believed to misuse the internet or technology in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Child Protection and Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Inappropriate Use by Children

Should a child be found to misuse the online facilities or technology whilst at school, the following consequences should occur:

- A Senior Leader will contact parents/carers requesting a meeting, where they will outline the breach where a child is deemed to have misused technology.

In the event that a child accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action.

Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child deliberately misusing online technologies should also

be addressed by the school.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

All online safety incidents must be logged on CPOMS using the Online Safety Incident Log.

Copyright and licensing

All software loaded on school computer systems must have been agreed with the Headteacher. It is a criminal offence to "pirate" software. Personal software should not be loaded to school computers under any circumstances. The school agrees to respect the intellectual ownership of software. Please refer to Copyright Designs and Patents Act 1988 and1991 European software Directive.

Templemoor Infant and Nursery School
Acceptable Use Agreement (AUA) for Staff and other Adults in school 2022/2023

This acceptable use agreement 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 school digital technology systems are primarily intended for educational use and that I will only use the systems for 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 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 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 the school:

- I will not use personal email addresses on the school ICT systems.
- 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, terrorist or extremist 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 use a USB device in school.
- 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 Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.

- I understand that data protection policy requires that any staff or 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 the 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 any online activity outside of school, including messages sent and posts made on social networking websites, must not bring my professional role or the name of the school into disrepute.
- I understand that if I fail to comply with this acceptable use 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.

Print name:	
Signed:	
Date:	

Templemoor Infant and Nursery School Acceptable Use Agreement for Parents and Children

Dear Parent/ Carer,

As part of the curriculum at Templemoor Infant and Nursery School, your child will be accessing the internet. In order to support the school in educating your child about online safety, the school has an Online Safety Policy available to view on the school website at templemoorinfants.co.uk under the tab 'Parents', 'Online Safety'.

This acceptable use agreement is intended to ensure:

- that children 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 about their on-line behaviour.

The school will try to ensure that children 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 agreement 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.

Parent/ Carer Permission Form

Parent/Carers Name: .....
Pupil Name:.....
As the parent/carer of the above child, I give permission for my child to have access to the internet and to ICT systems at school.

I understand that the school has discussed the acceptable use agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: .....
Date:

Templemoor Infant and Nursery School

Early Years Foundation Stage

Our rules for acceptable use of digital equipment and the internet.
These rules help us to enjoy using technology and they keep us safe.

- I will tell my teacher or suitable adult if I see something on the screen that I do not understand or that upsets me.
- I will ask a teacher or suitable adult if I want to use the computers/ tablets.
- I will only use the programs or websites that my teacher or suitable adult has said I can use.
- I will take turns sensibly with the computer/ tablets and other equipment.
- I will take care of computers/ tablets and other equipment.
- I know that if I break the rules I might not be allowed to use a computer/ tablet.

Signed

(child):……

Date:…… ***Please return to your class teacher.***

Templemoor Infant
And Nursery School

Key Stage One

Our rules for acceptable use of digital equipment and the internet. These rules help us to enjoy using computers and they keep us safe.

- I will ask a teacher or suitable adult if I want to use computer equipment.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will tell an adult if I see something unexpected or that upsets me on the screen, either at school or at home.
- I will tell an adult about any upsetting or 'cyberbullying' messages sent to me, even if it only happens once.
- I will not 'cyberbully' others.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will always be very careful when using computers and digital equipment.
- If I am not careful I will not be able to use the digital equipment or the internet.
- I will not click on keys or links if I don't know what they do.
- I know and understand that not all information online is true.
- If I break these rules I will not be able to use technology or the internet in class.

Signed

(child):……
……

Date:…… ***Please return to your class teacher.***

Templemoor Infant and Nursery School: Online safety incident reporting log

Details of all online safety incidents to be recorded by staff and passed to the Designated Safeguarding Lead. These records will be stored on CPOMS.

Date/time	Incident	Action Taken	Incident Reported by	Signature
		What? By Whom?		