Templemoor Infant and Nursery School

e-safety Policy

Policy Adopted	7th October 2017
Committee	Resources and Safety Committee
Last Reviewed	27th February 2020
Next Review Date	February 2022

Templemoor Infant and Nursery School

e-safety Policy

Due to the ever changing nature of digital technologies, this E-Safety Policy 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 e-safety or incidents that have taken place. This Policy has been written using guidance from SWGfL and 360 Degree Safe.

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 e-safety roles and responsibilities of individuals and groups within the school.

The Governing Body

Governors are responsible for the approval of the E-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 e-safety incidents and monitoring reports.
The Governor responsible for E-Safety is Mrs Judith Davenport. The role of the E-Safety Governor includes:

- regular meetings with the Designated E-Safety Lead, Mr Stuart Hodgson
- regular monitoring of e-safety incident logs
- regular monitoring of filtering logs
- reporting to relevant Governors

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including e-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 e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse".
- The Senior Leadership Team will receive regular monitoring reports from the Designated Safeguarding Lead.

Online Safety Lead/ Designated Safeguarding Lead

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

- leads on e-safety issues
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-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 e-safety incidents via CPOMS and regularly reviews the log of incidents to inform future e- safety developments
- meets regularly with the E-Safety Governor to discuss current issues and to review incident logs and filtering logs
- reports to the Resources and Safety committee

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:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
- that 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 e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Designated Safeguarding Lead for investigation/action/sanction.
- that 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 e-safety matters and of the current school e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Agreement (AUP).
- 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.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- children understand and follow the e-safety and acceptable use agreements.
- 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 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 Policy 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 e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Discuss e-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 e-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 Policy 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 e-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.

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.

Education – Children

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 termly e-safety-related lessons in every year group as part of the Computing and PHSE curriculum.
- We will celebrate and promote e-safety through assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-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 Policy 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.

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 e-safety talks and training, linking with Moorlands Junior School when possible.
- Include useful links and advice on e-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 e-safety on the school website with links to relevant e-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 e-safety knowledge and experience. This may be offered through the following:

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

Education & Training – Staff/Volunteers

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

- A planned programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-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 E-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 e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-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.
- Participation in school training/information sessions for staff or parents.

Technical – Infrastructure/ equipment, filtering and monitoring

The school will be responsible for ensuring that access to the ICT systems 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. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Internet filtering/monitoring should 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 incident/security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, 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 Policy (AUP) 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 e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. We will regularly review our Internet access.

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

Using Digital Images, Videos and Sound

- Digital images, video and sound created on the school premises will only be created using equipment provided by the school, with the exception of school plays, assemblies and concerts where parents written permission has already been obtained in advance.
- Staff will follow the school Social Media Policy on the use of photographs, videos, mobile phones and social networking sites.

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 e-safety point of view.
- We will regularly amend the e-safety policy to reflect any new technology that we use, or to reflect the use of new technology by children which may cause an e-safety risk.

Data Protection

The school ensures that:

- It has a Data Protection Policy in place and that this is reviewed regularly.
- 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
- can 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

The school website

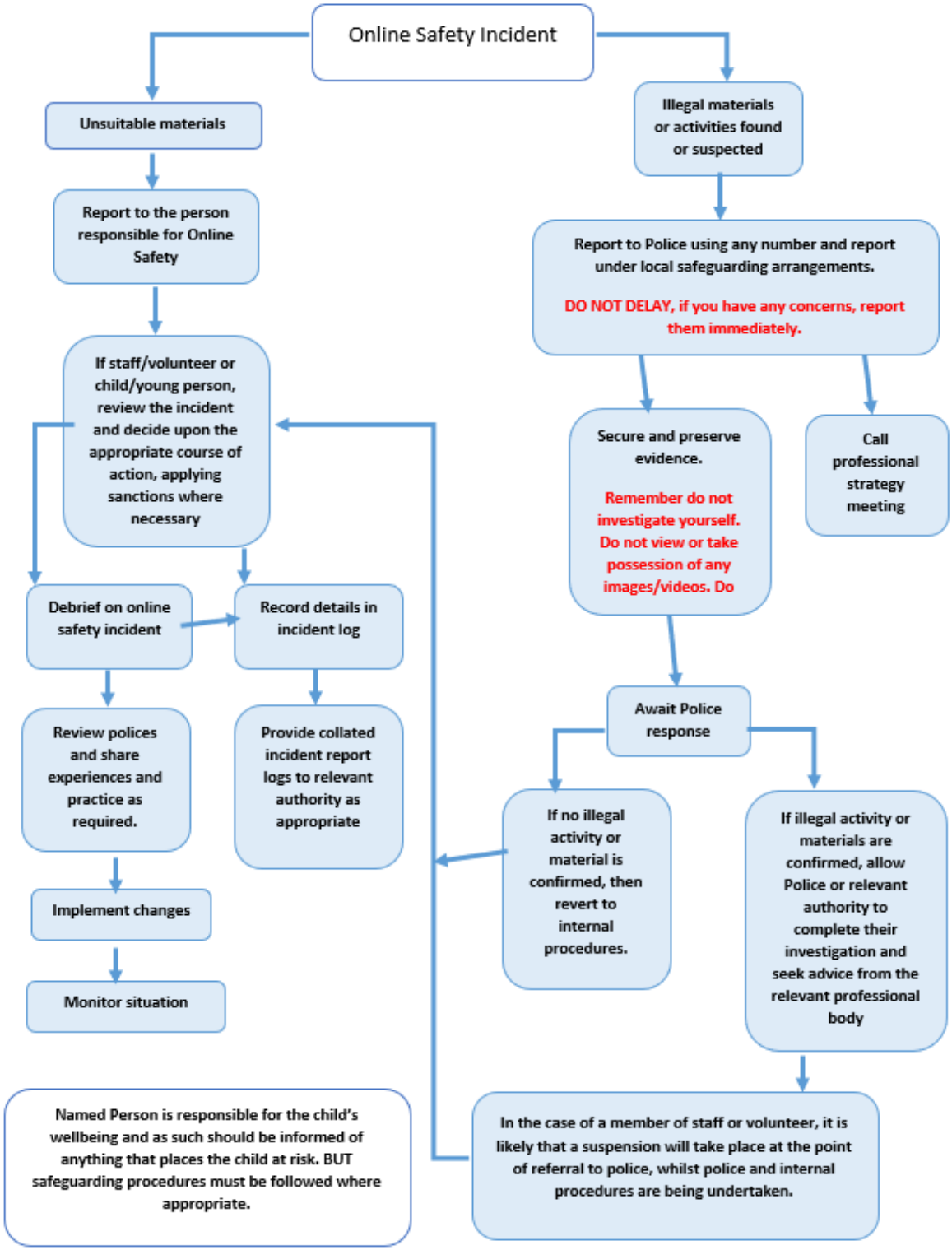
- The school website will not include the personal details, including individual e-mail addresses or full names of children.
- All content included on the school website will be approved by the Head teacher, or class teachers before publication.
- Permission from parents will be sought before any photographs 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.

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 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.



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

- 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 Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Inappropriate Use by Children

Should a child or young person 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 in Safeguarding Policy where a child or young person is deemed to have misused technology.

In the event that a child or young person 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 or young person 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 or young person deliberately misusing online technologies should also be addressed by the establishment.

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 e-safety incidents must be logged on CPOMS using the E-safety Incident Log.

Copyright and licensing

All software loaded on school computer systems must have been agreed with the Head and School Business Manager. 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 Policy for Staff and other Adults in school
2021/2022

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the ICT systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school ICT equipment at other locations such as your home.

- Any use of school ICT systems will be for professional purposes only.
- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g. by logging in for them.
- Any online activity should not harass, harm, offend or insult other users.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow the school's procedure and report this immediately.
- You should not download or install any hardware or software without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.
- The use of USB drives is not permitted.
- Any electronic communications should be related to schoolwork only, and should be through school e-mail addresses or other school systems e.g. learning platforms. It is not acceptable to contact children using personal equipment or personal contact details, including your own mobile phone or through your personal social network profiles.
- Any online activity, including messages sent and posts made on social networking websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.
- Any still or video images of children and staff should be for professional purposes only. They should be taken on school equipment only, and stored and used onsite. Such images should not be taken off-site without permission and valid reason.
- All personal electronic devices (e.g. mobile phones) will not be used in the presence of children, except in an emergency.
- You will not give out your personal details, or the personal details of other users, to children or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children or parents.
- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
- Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.
- You should support and promote the school e-safety Policy, and promote and model safe and responsible behaviour in children when using ICT to support learning and teaching.

- Finally, you understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others.

I understand that if I do not follow all statements in this AUP and in other school policies I may be subject to disciplinary action in line with the school's established disciplinary procedures.

Print name:	
Signed:	
Date:	

Templemoor Infant and Nursery School
Acceptable Use Policy for Children

Dear Parent or 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 e-safety (safe use of the Internet), the school has an e-safety Policy available on to view on the school website at templemoorinfants.co.uk

Please read and discuss our 'Acceptable Use Policy for Children' with your child and sign and return the form to school. Please support us in helping to keep your child safe. Should you wish to discuss this matter further, please do not hesitate to contact the school.

Yours sincerely

Mr Stuart Hodgson

Headteacher

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 an adult if I see something on the screen that I do not understand or that upsets me.
- I can use the computer, iPads and other equipment in free play.
- I will only use the programs or websites that my teacher has said I can use.
- I will take turns sensibly with the computer and other digital equipment.
- I will always be very careful using computers and digital equipment.
- If I break these rules I will not be able to use the computers in free play.

Signed (child):……

Signed (parent/carer):……

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):……

Signed (parent/carer):……

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

Templemoor Infant and Nursery School: E-safety incident reporting log

Details of all e-safety incidents to be recorded by staff and passed to the Designated Safeguarding Lead.

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