Thorney Island Community Primary School Online Safety Policy

Introduction

At Thorney Island Community Primary School, we feel that the internet and other technologies have an important role to play in the learning and teaching process and supporting achievements in all areas of a child's life while in education and beyond into adulthood. Thorney Island Community Primary School is committed to providing all children with opportunities to develop their computing knowledge, skills and understanding confidently, competently and safely in their learning and in everyday contexts. Children are encouraged to become independent and astute users of technology, recognising both opportunities and risks and using strategies to stay safe. This Online Safety Policy reflects the school's commitment to their safeguarding and well-being.

Responsibilities of the School Community

We believe that Online Safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Leadership Team

- Develop and promote an Online Safety culture within the school community.
- Support the Online Safety lead in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to Online Safety effectively.
- Receive and regularly review Online Safety incident logs (See Appendix B) and be aware of the procedure to be followed should an Online Safety incident occur in school. (See Appendix A)
- Take ultimate responsibility for the Online Safety of the school community.

Responsibilities of the Online Safety Lead (Mr Stamp)

- Promote an awareness and commitment to Online Safety throughout the school.
- Be the first point of contact in school on all Online Safety matters.
- Create and maintain Online Safety policies and procedures.
- Develop an understanding of current Online Safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in Online Safety issues.
- Ensure that Online Safety education is embedded across the curriculum.
- Ensure that Online Safety is promoted to parents and carers at least annually and in response to current events or issues.
- Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on Online Safety issues to the SLT and governors as appropriate.
- Ensure an Online Safety incident log is kept up-to-date.
- Keep up to date with new technologies and their potential for inappropriate use by pupils and staff.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's Online Safety policies and guidance.
- Read, understand and adhere to the school staff AUP (Acceptable User Policy).
- Develop and maintain an awareness of current Online Safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed Online Safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an Online Safety incident occurs. (See Appendix A)
- Maintain a professional level of conduct in their personal use of technology at all times.
- Be aware of and alert to the potential signs of online grooming and child sexual exploitation.
- Remind children of the AUP at the start of every school year and/or when necessary.

Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the school's Online Safety policies and guidance.
- Read, understand and adhere to the school staff AUP.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Take responsibility for the security of the school IT system.
- Report any Online Safety-related issues that come to your attention to the Online Safety Lead.
- Develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to your work.
- Liaise with the local authority and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

- Read, understand and adhere to the school pupil AUP. (This is part of each child's induction pack when they start school)
- Help and support the school in creating Online Safety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies in school and at home.
- Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Discuss Online Safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting Online Safety.
- Read, understand and promote the school pupil AUP with your children.

- Take responsibility for learning about the benefits and risks of using the internet and other technologies that your 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 your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

- The school has appointed a member of the governing body to take lead responsibility for Safeguarding.
- Read, understand, contribute to and help promote the school's Online Safety policies and guidance.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an overview of how the school's IT infrastructure provides safe access to the internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online Safety activities.
- Ensure appropriate funding and resources are available for the school to implement their Online Safety strategy.

Responsibilities of Adult or Community Education Training Staff

- Develop and promote an Online Safety culture within the school community.
- Support the Online Safety Lead in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to Online Safety effectively.
- Read, understand and help promote the school's Online Safety policies and guidance.
- Read, understand and adhere to the school staff and other adults AUP.
- Develop and maintain an awareness of current Online Safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed Online Safety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Be aware of what to do if an Online Safety incident occurs. (See Appendix A)
- Maintain a professional level of conduct in their personal use of technology at all times.

Teaching and Learning

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

- We will provide a series of specific Online Safety-related lessons in every year group as part of the Computing Curriculum, PSHE Curriculum and other lessons.
- We will celebrate and promote Online Safety through whole-school and individual class activities.
- We will discuss, remind or raise relevant Online Safety messages with pupils routinely or whenever suitable opportunities arise during lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- Staff will also model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

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:

- Include useful links and advice on Online Safety regularly in newsletters and on our school website.
- Include a section on Online Safety in the School Prospectus.
- Ask parents to read the Acceptable User Policy, discuss it with their children and sign it.
- Provide up-to-date training/advice on how to keep children safe online at home e.g. through newsletters.

Managing IT Systems and Access

Internet access is provided by Exa Networks who ensures that access is a safe as possible. The school infrastructure, hardware and software are managed by JSPC.

- The school will be responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.

- All users will sign the 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 IT systems, and that such activity will be monitored and checked.
- At KS1 pupils will access the computers using a class log-on, which the teacher supervises. All internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.
- At KS2 pupils will access the computers using a class log-on. Internet access will be supervised by a member of staff.
- Members of staff will access the internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the internet through their log-on. They will abide by the school AUP at all times.
- Members of staff will use only school USB drives/hard drives to transfer data between school and teacher laptops. Laptops should be password protected to prevent loss of confidential data.
- Any administrator or master passwords for school IT systems should be kept secure and available to at least two members of staff, e.g. head teacher, bursar and member of technical support.
- 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 will regularly audit IT 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 provision, and review new methods to identify, assess and minimize risks.

Filtering Internet Access

- The school uses a filtered internet service. The filtering is provided through Exa Networks and is password protected.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety Lead.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead. The school will report this to appropriate agencies which may include the filtering provider, LA, CEOP and/or the police.
- The school infrastructure, hardware and software is managed by JSPC.

User Actions

Learning technologies in school

	Pupils	**Staff**
Personal mobile phones brought into school	Allowed with permission. (Kept in school office)	Allowed
Mobile phones used in lessons	Not allowed	Not allowed
Mobile phones used outside of lessons	Not allowed	Allowed at certain times
Taking photographs or videos on personal equipment	Not allowed	Not allowed
Taking photographs or videos on school devices	Allowed	Allowed
Use of hand-held personal MP3 players or personal gaming consoles	Not allowed	Allowed at certain times
Use of personal tablets and smart watches with access to the internet	Not allowed	Allowed at certain times
Use of personal email addresses in school	Not allowed	Allowed
Use of school email address for personal correspondence	Not allowed	Discouraged
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services	Not allowed	Not allowed
Use of blogs, augmented reality, podcasts	Allowed	Allowed
Use of video conferencing or other online video meetings	Allowed with supervision	Allowed (if using with children, must be agreed by member of SLT and online safety lead)
Use of social networking sites	Not allowed	Not allowed

Using Email and Social Networking in and outside school

- Staff should use approved e-mail accounts allocated to them by the school and be aware that their use of the school e-mail system can be monitored and checked if deemed necessary.
- Pupils are not permitted to access personal e-mail accounts in school.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.
- Staff using social networking sites are not to have any contact with anyone under the age of 18 who they know through a work capacity.

School staff should ensure that:

- No reference is made in social media to pupils, parents/carers or school staff.
- Staff should 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 official school social media accounts:

- Posts have to be approval by senior leaders
- There is a clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- The users of the school account must adhere to this policy.
- This policy allows for reporting and dealing with abuse and misuse of such accounts.

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 school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Using images, video and sound

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will only be created using equipment provided by the school.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff or pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

Using social networking, augmented reality, podcasts, and other ways for pupils to publish content online

We may use blogs, wikis, podcasts or other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Pupils will model safe and responsible behaviour in their creation and publishing of online content. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Pupils and staff will not access social networking sites in school.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using mobile phones

- Personal mobile phones will not be used during lessons by pupils or staff. This includes the use of smart watches.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, they should do so via school.
- Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Using new technologies

- As a school we will keep abreast 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 pupils which may cause an Online Safety risk.

Protecting personal data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the head teacher, and without ensuring such data is kept secure.

The school website and other online content published by the school

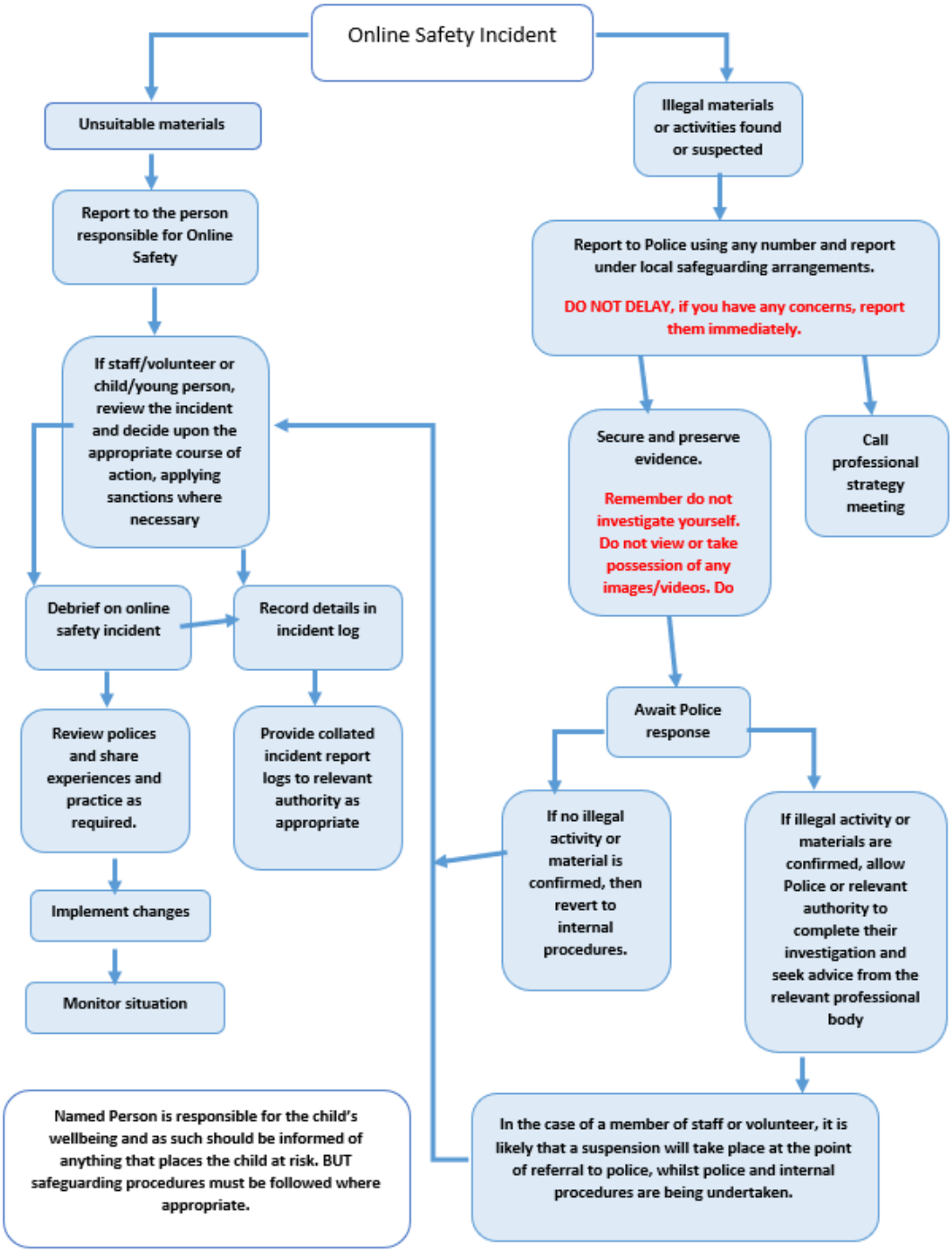
- The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
- A generic contact e-mail address will be used for all enquiries received through the school website for the school office and SENCo.
- The school website will not include photographs of any children where parents have specifically asked for their exclusion.
- The school website will not include photographs of staff without prior permission.

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

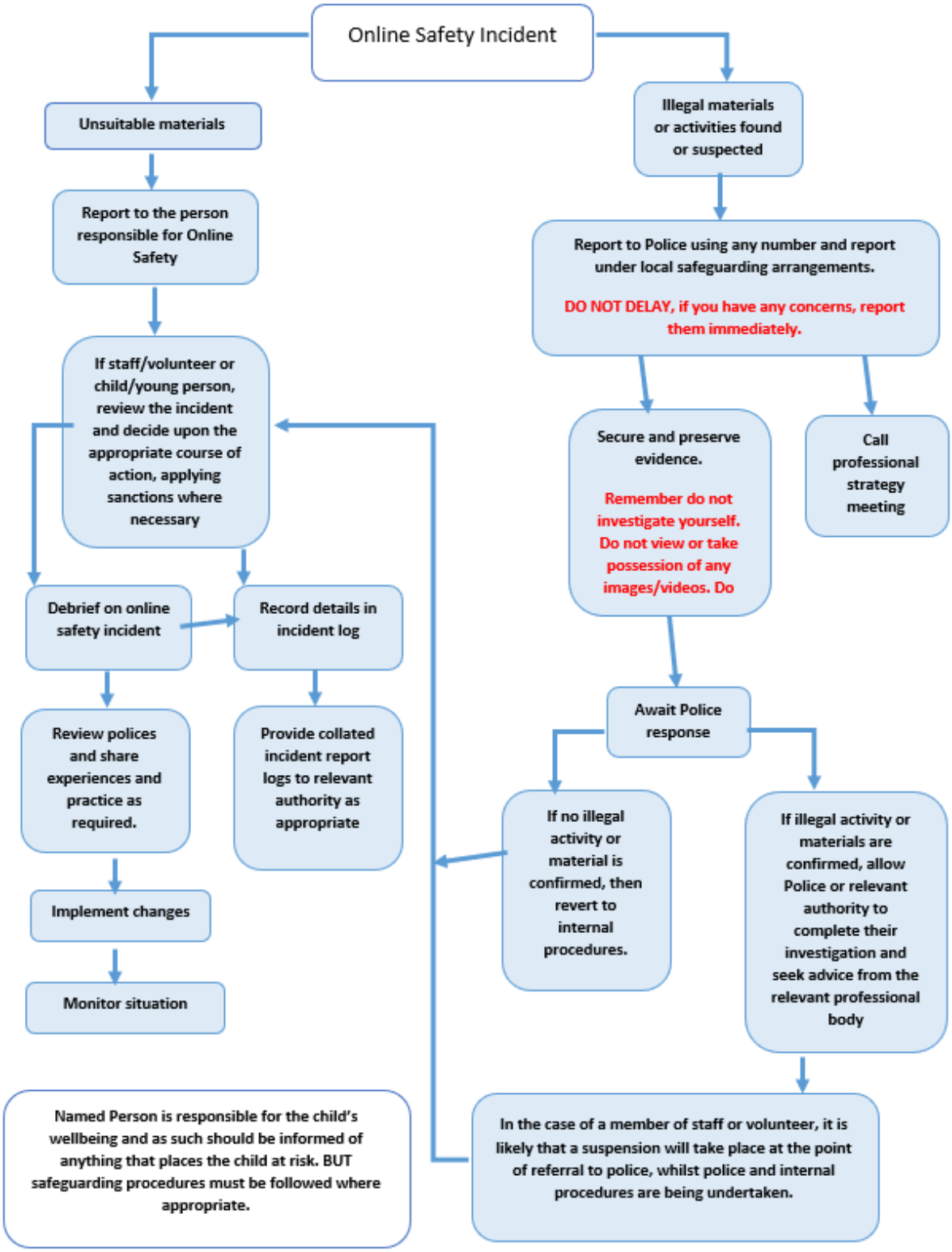
It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff / volunteer 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
    - 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 school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix A – Online Safety Incident Flowchart



Appendix B – Online safety incident report form.

Incident; What? When? Who? Where?	Date
Follow up/action taken:	
Follow up/action taken:	
Follow up/action taken:	
Follow up/action taken:	