Online Safety Policy

Online safety is an integral part of safeguarding. This policy sets out our approach to online safety to empower, protect and educate learners and staff in their use of technology. It establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate

Version number	1.1
Consultation groups	Trust Online Safety Lead and Head teacher
Approved by	
Approval date	January 2023
Implementation date	January 2023
Policy/document owner	School Online Safety Lead
Status	Statutory
Frequency of review	1 Years
Next review date	September 2023
Applicable to	All Discovery Schools

Document History

Version	Version Date	Author	Summary of Changes
V1.0	9th September 2021	Adam Lapidge – Online Safety Lead	New policy prepared in line with: • Keeping children safe in education - September 2021 • Working Together to Safeguard Children, 2018 • Ofsteds Review of Sexual Abuse and Colleges – June 2021
V1.1	September 2022	Zack Minton Head of Safeguarding	Policy updated and prepared in line with: □ Keeping children safe in education September 2022 Adoption to be compliant with Keyham Lodge School practice

Contents

1. Statement of Intent

Keyham Lodge School fully recognises the contribution it can make to protect children and support pupils in school. The online safety policy is intended to demonstrate the organisation's commitment to:

- Ensuring the safety and wellbeing of children, young people and adults is paramount when using the internet, social media or mobile devices.
- Providing staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensuring that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all members of Discovery Trust including staff, pupils, advisory board members, volunteers, parents, carers, visitors, and community users who have access to and are users of Trust digital technology systems, both in and out of the Trust.

2. Linked policies

This policy statement should be read alongside our organisational policies and procedures, including:

- Acceptable Use policy
- Anti-Bullying Policy (including Cyberbullying)
- Document Retention Management Policy
- GDPR Data Protection Strategy
- Mental Health and Wellbeing Policy
- Mobile Phone and Smart technology policy
- RSE and Health Education Policy
- Safeguarding and Child Protection Policy
- Pupil Behaviour Policy
- Social Media Policy
- Special Educational Needs and Disability Policy
- Home Learning Protocol Policy

Staff related Policies and Procedures:

- Acceptable Use policy
- Disciplinary Policy and Procedure
- Mobile Phone and Loaned Property Policy
- Staff handbook which includes Staff Code of Conduct
- Staff Wellbeing Policy
- Trust Platform Working document

The above list is not exhaustive but when undertaking development or planning of any kind the school will consider the implications for online safety.

3. Key Roles and Responsibilities

The school takes a whole-school approach to online safety and all stakeholders are responsible for ensuring that effective policies and procedures are maintained and upheld. It is expected that all staff and volunteers read and understand this policy and implement it consistently.

3.1 Governance

Trustees and Advisory Board Members and play an important part in monitoring the online safety provision across the trust and within schools. They have a responsibility to keep up to date with online safety by receiving appropriate online safety training (delivered by Trust Online Safety Lead).

The Trust Board is responsible for:

- Reviewing and approving this policy.
- Monitoring the effectiveness of the policy at a Trust level by reviewing data and reports from the Trust Online Safety Lead and Trust Safeguarding Lead.
- Appointing a designated Trustee with oversight of safeguarding and online safety at a trust level. It is the role of the lead trustee to meet with the Trust Safeguarding Lead regularly to ensure any weaknesses are addressed.
- Agreeing and adhering to the terms on acceptable use of the Trust's ICT systems and the internet.
- Developing individual knowledge and understanding to ask the right questions and professionally challenge and test what happens in schools and across the Trust.

The School Advisory Board is responsible for:

- Adopting this policy locally ensuring it meets the needs the school.
- Monitoring the effectiveness of the policy at a school level by monitoring data and audit reports for the Trust Online Safety Lead and Trust Safeguarding Lead.
- Appointing a designated Advisory Board Member with oversight of safeguarding and online safety at a school level. It is the role of the lead Advisory Board Member to meet with the school Safeguarding Lead regularly to ensure any weaknesses are addressed.
- Agreeing and adhering to the terms on acceptable use of the Trust's ICT systems and the internet.
- Developing individual knowledge and understanding to ask the right questions and professionally challenge and test what happens in school.

3.2 Trust Online Safety Lead

The role of Online Safety lead forms part of the Trust's safeguarding team. The Trust Online Safety Lead will receive regular training on online safety and be aware of the potential for serious child protection and/or safeguarding issues that may arise from the online world. They will have overall oversight of the trust's online safety strategy.

Key responsibilities:

- Delivering training trust-wide to school online safety DSLs
- Monitoring online safety in schools through yearly audits*

□

Ensuring support mechanisms are in place for schools dealing with complex situations.

- Regularly updating trust leaders on the progress made with online safety, as well as reporting data to the trust board.
- Ensuring that there are robust protocols in place for both monitoring and reporting online safety issues.
- Ensuring all staff adhere to the policies and procedures around online safety. E.g. acceptable use policies and loan equipment agreements.
- Responsible for actioning the annual review of the online safety policy.

*The Trust Online Safety Lead will use the SWGFL 360 Safe audit as part of its yearly online safety audit. Details of this can be found here: https://swgfl.org.uk/products/360-degreesafe/

The purpose of these audits is to ensure the school continues to:

- Review and develop its online safety strategy.
- To find and action any areas of development within the school online safety programme.
- To work towards achieving/renewing the Online Safety Mark

3.3 Head Teachers/Head of Schools and SLT

Head teachers / Head of school and members of SLT take overall responsibility in ensuring that all staff and pupils understand and follow the policies and procedures of online safety.

Key responsibilities:

- To liaise with the Online Safety DSL about the development of the school's online safety strategy.
- Support the Online Safety DSL in carrying out their role.
- Review the online safety curriculum with the Online Safety DSL.
- Share the online safety audit report and actions to the Advisory Board.
- To know the procedures in the event of serious online safety allegations against a member of staff.
- Responsible for ensuring the Online Safety Lead is given time to receive suitable training to support them in their role.
- Ensure all staff understand this policy and that it's implemented consistently.
- Reviews the school's infrastructure/network with the Director of IT or Senior Technician to ensure it is safe and fit for purpose.

3.4 School Online Safety Lead

This role will be part of the school's Designated Safeguarding Lead team. The Online Safety DSL will be trained on online safety issues and be aware of the potential for serious child protection/safeguarding issues.

Key responsibilities:

□

- Responsibility for online safety issues in school.
  Liaise with Trust Online Safety Lead on the school's online safety development and strategy.
- Liaise with external agencies where necessary.
- Provide regular reports on online safety in school to the headteacher/head of school.
- Keep up to date with current legislation, developments, and resources.
- Provide training and advice for all staff across school.
- Lead role in personalising policies/documents.
- Attends any relevant meetings with Advisory Board members and updates them on progress of online safety.
- Ensure pupil voice is considered as part of online safety development/strategy.
- Liaise with the Trust in the event of serious incidents.
- Ensure all online safety incidents are logged onto CPOMs, providing training for staff where necessary.

3.5 School IT Technicians

School IT technicians are the first line of defense against online safety, and they play a huge role in ensuring that pupils and staff are kept safe.

Key responsibilities are to:

- Ensure that school networks are secure and safe to use.
- Regularly monitor school networks and internet.
- implement and update monitoring software/systems are as requested by Trust's senior technical team.
- Ensure that only authorised users can access the network and these users adhere to the trust's password policy.
- Ensure that they keep up to date with relevant online safety updates.
- Ensure that filtering policies are applied to the correct users.
- Ensure that any filtering request changes are liaised and agreed with head teachers / SLT before actioning.
- Ensure that any online safety incidents are sent to class teachers and SLT for actioning.

3.6 Teaching and Support Staff

Teachers and support staff are the day-to-day contact for pupils and therefore responsible for promoting safe online safety behaviour.

Key responsibilities are to:

- Ensure they attend any relevant training that is issued by the Head teacher or Online Safety DSL.
- Ensure that they adhere to the policies and procedures relating to online safety. E.g., acceptable use policy, loan agreement form, staff handbook.

□

- Support pupils understanding and ensure they follow online safety procedures and policies.
- Ensure that where there is pre-planned internet use, pupils are guided to sites that are suitable.
- Report any online safety concerns to the online safety DSL.
- Ensure policies around mobile phones are enforced with all pupils.

  Ensure digital communications with pupils/parents/carers on carried out using official school systems and that conversations always remain professional.
- Ensure they deliver the online safety curriculum to all pupils.
- Ensure online safety issues are embedded into all aspects of the curriculum.

3.7 Pupils

Pupils are responsible for:

- Ensuring that they use the digital technology systems in accordance with the pupil acceptable use policy.
- Understanding the importance of reporting abuse, misuse or access to inappropriate material.
- Adhering to the school mobile phone policies and are aware of the consequences if they don't follow this.
- Understanding the need for good online safety behaviour both in and out of school.
- Providing valuable feedback about online safety through surveys and discussions.

3.8 Parents/carers

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

- Digital and video images taken at school events.
- Online learning platforms (Microsoft Teams) by following the Home Learning Protocol Policy.
- Their children's personal devices in the school/academy (where this is allowed).

3.9 Community Users

Community users who have access to the school systems or programmes as part of the wider school provision will be expected to sign a Community User Acceptable Use Policy/Agreement before being provided with access to school systems. This will be done as they enter the building using our signing in system.

□

4. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Online Safety Designated Safeguarding Lead has overall responsibility for the school's approach to online safety, with support from the school's senior leadership team, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training.
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation.
- Online safety is integrated into learning throughout the curriculum.
- Assemblies are conducted termly on the topic of remaining safe online.

5. Online safety in the curriculum

We want our pupils to take responsibility and act in a responsible way.

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

Online safety will be provided in the following ways:

- Pupils are taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will 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. Schools are required to ensure all devices have monitoring software on them that detects and alerts the school of any potential exposure to extremism.
- Pupil's will be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies, the internet, and mobile devices.
- In lessons where internet use is pre-planned, staff will do their best to ensure that students/pupils are 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and be agreed by the school's Head teacher/SLT before actioned by the technical team.

6. Training

6.1 All staff

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

- A planned programme of formal online safety training is made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff 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 Online Safety Lead will receive regular updates through attendance at external training events or as part of internal training from the Trust's Online Safety Lead.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- Staff are expected to read and understand the trust's platform working document which outlines the safe use of applications and platforms with pupils.

6.2 Trust Online Safety Lead DSL

It is essential that the Trust Online Safety Lead DSL receives additional training to support them in their role. This training will be done by:

- Attending advanced online safety training DSL training on an annual basis.
- Participating in online safety expert groups (SWGfL 360 Safe Assessor Programme).
- Attending expert external training sessions through various providers.
- Keeping up to date with latest legislation and policy changes.

6.3 Trustees and Advisory board members

Advisory Board members/trustees take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This will be offered through:

 Participation in Trust training sessions delivered by the Online Safety Lead.

7. Online safety concerns

7.1 Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom

- Unpleasant messages sent via instant messaging apps (e.g. WhatsApp)

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

7.2 Peer on peer abuse

Pupils may use the internet and technology as a vehicle for sexual abuse and harassment. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

The school will respond to all concerns regarding online peer-on-peer sexual abuse and DSLs will investigate the matter in line with their Child Protection and Safeguarding Policy.

7.3 Grooming

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online where the perpetrator will often hide their identity through pretending to be someone they are. Pupils are less likely to report grooming behaviour because:

- The pupil believes they are talking to another child
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

7.4 Child sexual exploitation (CSE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CSE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

7.5 Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

7.6 Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and ‘booting’, which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime.

Where there are any concerns about a pupil’s use of technology and their intentions about using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

8. Responding to online incidents

8.1 Responding to pupil incidents

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The schools DSLs will determine the seriousness of all incidents and report all illegal activities/incidents to the appropriate organisation, these include:

- Police
- CEOP (child exploitation and online protection)
- CyberChoices

8.2 Responding to staff incidents

Where a staff member misuses the school's IT systems or internet or uses a personal device in a way that their actions constitute in misconduct, then the matter will be dealt with in accordance with the staff disciplinary procedure. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police. A flow chart in dealing with illegal activity (appendix 2) supports the school in taking the correct action.

9. Technical Systems

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that internet filtering is actively monitored for misuse. A full description of our policies are procedures relating to our technical systems can be found in Annex 1: Technical Systems

10. Remote learning

All remote learning is delivered in line with the school's Home Learning Protocol Policy. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, senso-monitoring software installed, has working audio and video and can download documents where appropriate. The school is not responsible for ensuring that devices that go home have strict filtering installed and this is the responsibility of the parent/carer to ensure safe use. During the period of remote learning, the school will maintain regular contact with parents to: Reinforce the importance of children staying safe online.

11. Policy review

This policy will be reviewed by the Trust Online Safety Lead annually and updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation. A formal review will be completed every two years for Trust Board approval.

Appendix 1: Pupil Acceptable Use Policies

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

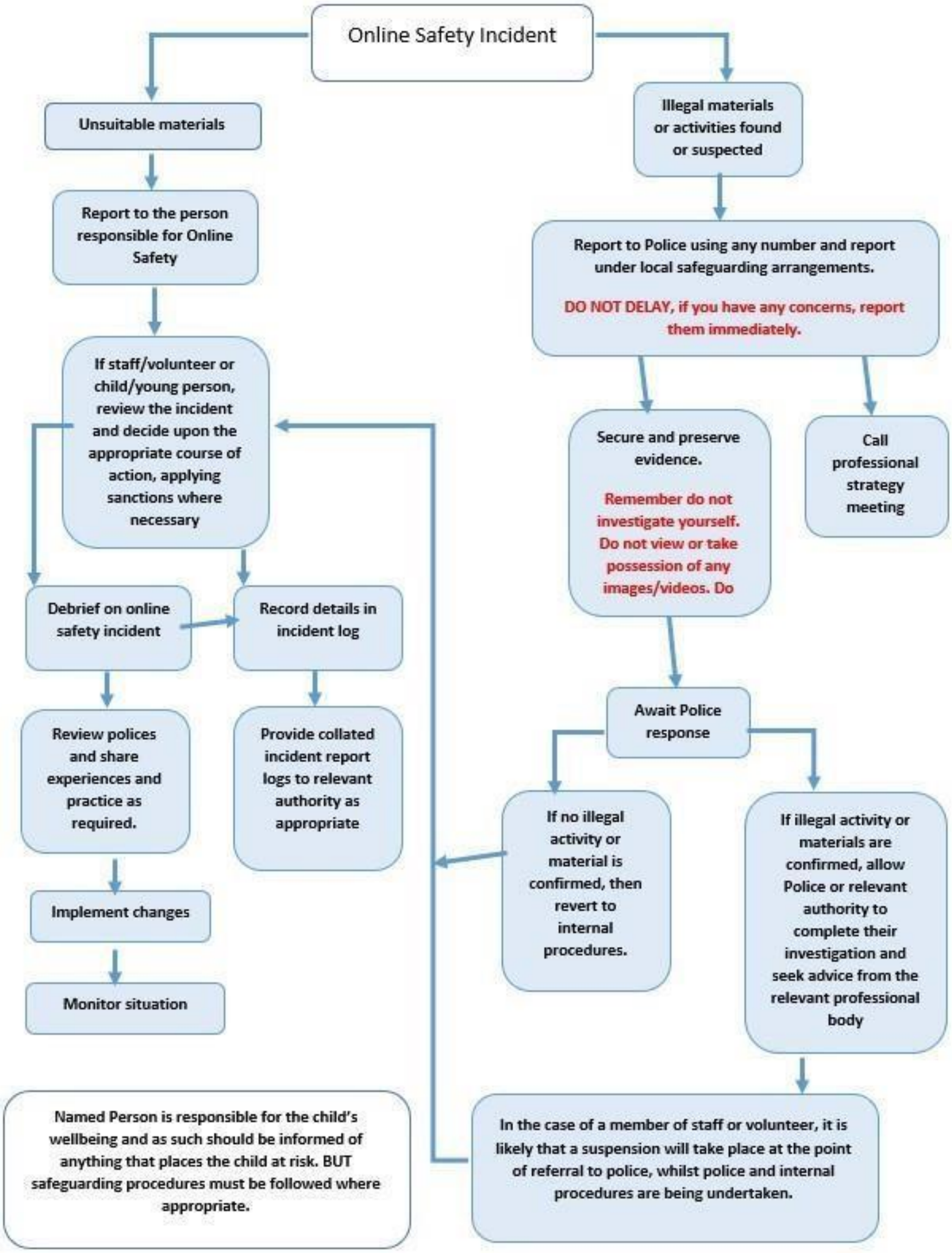
When using the school's ICT systems and accessing the internet in school, I will:

- Use them for a schoolwork or homework
- Use them only with a teacher being present, or with a teacher's permission
- Not access any inappropriate websites
- Not access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Never use chat rooms
- Only videoconference call with a teacher present
- Never open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use only kind and appropriate language when communicating online, including in emails
- Never share my password with others or log in to the school's network using someone else's details
- Never give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Never arrange to meet anyone offline without first telling my parent/carer, or without an adult to accompany me

Signed (Pupil):

Date:

Appendix 2: Staff online safety incident flow-chart



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.