Pitmaston Primary School Online Safety Policy

Due to the ever changing nature of digital technologies, this policy is reviewed at least annually by the Governing Body. The Governing Body has delegated responsibility to the Headteacher to update this policy in line with DfE changes to safeguarding practice.

Signature L M Townsend **(Chair of Governors)**

Print Name: Lynda Townsend

Date: 03.07.2025

Approved by:	Governing Body	**Date:** 03.07.2025
Last reviewed on:	03.07.2025	
Next review due by:	Summer term 2026	

Safeguarding Statement

Pitmaston Primary School recognise our moral and statutory responsibility to safeguard and promote the welfare of all pupils. We endeavour to provide a safe and welcoming environment where children are respected and valued. We are alert to the signs of abuse and neglect and follow our procedures to ensure that children receive effective support, protection and justice, including any online abuse. Child protection forms part of the school's safeguarding responsibilities. Please also see our Early Help Offer which can be found on the school website. http://www.pitmaston.co.uk/about-us/

Key Personnel: The Designated Safeguarding Lead (DSL) is: Sara Bream, Deputy Headteacher

Contact details: email: sbream@pitmaston.worcs.sch.uk Telephone: 01905 423710

The Deputy DSL(s) are: Kate Wilcock (Headteacher) Jane Lyons (Assistant Headteacher) Sue Bladen (School Business Manager) Rebecca Williams (Phase Leader for UKS2) Contact details: Telephone: 01905 423710

The nominated safeguarding governor is: Lynda Townsend

Contact details: email: ltownsend@pitmaston.worcs.sch.uk Telephone: 01905 423710

The Headteacher is: Kate Wilcock email: office@pitmaston.worcs.sch.uk Telephone: 01905 423710

The Chair of Governors is: Lynda Townsend email: ltownsend@pitmaston.worcs.sch.uk Telephone: 01905 423710

Other named staff and contacts:

- Designated Teacher for Looked After Children: Jane Lyons (Assistant Headteacher)
- Safeguarding in Education Adviser, WCC: Denise Hannibal
- Local Authority Designated Officer/Position of Trust: John Hancock
- Family Front Door: 01905 822666 (core working hours) Out of hours or at weekends: 01905 768020

This online safety policy has been developed by a working group made up of:

- Headteacher and senior leaders,
- Online Safety Leader.
- Computing Curriculum Leader
- Staff – including teachers, support staff, technical staff
- Governing Body
- Parents and carers

Governors' Committee Responsible: Full Governing Body

Governor Lead: Lynda Townsend

Designated Safeguarding Lead of Staff: Sara Bream

Online Safety Lead: Rachel Harber Computing Curriculum Leader: Georgia Richardson

Status & Review Cycle: Statutory Annual Next Review Date: Autumn 2025

Overview:

Our online safety policy considers all current and relevant issues, and links with other relevant policies, including our child protection, behaviour and anti-bullying policies and in line with KCSIE 2024.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in Pitmaston are bound. Through our Online Safety Policy, we ensure we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

Contents

1. Aims

Our school will:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure that school has robust filtering and monitoring systems and processes in place in line with KCSIE 2024.
- Ensure that all staff receive appropriate safeguarding and child protection training, including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their induction. (KCSiE 24)
- Ensure all staff and Governors receive regular safeguarding and child protection updates including Online safety and cyber security

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying
- cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Meeting digital and technology standards in schools and colleges
- Sharing nudes and semi nudes

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

We are aware that, technology, and risks and harms related to it, evolve and change rapidly. Pitmaston Primary School will therefore carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. We will continue to use the online safety self-review tool for schools (360 safe Audit) in order to do this.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff namely the DSL and Online Safety Leader, Rachel Harber, to discuss online safety, and monitor online safety logs.

The governor who oversees online safety is Lynda Townsend.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the school's Acceptable Use Policy (Appendix 3)
- Ensure all staff undertake appropriate online safety and cyber security training
- Ensure that the online safety and computing curriculum teaches children to effectively keep themselves and others safe online
- Ensure sufficient resources are available through effective budget planning to keep the school network infrastructure, filtering and monitoring up to date
- Ensure that, as part of the requirement for staff and children to undergo regular updated safeguarding training, including in relation to online safety, that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning. (KCSiE 2024)

3.2 The Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead, Rachel Harber.

The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.

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

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL) and Online Safety Lead

The DSL will support the Online Safety Leader who will take a lead responsibility for online safety in school, in particular by:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, network manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged appropriately and dealt with in line with the school behaviour policy and safeguarding procedures
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body
- Understand the filtering and monitoring systems and processes in place

This list is not intended to be exhaustive.

3.4 The Online Safety Lead

Rachel Harber is Pitmaston's named Online Safety Leader. Her responsibilities include that she:

- Leads the Online Safety Group. (DSLs, Governors, Staff)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents with support and guidance from the DSL. (Sara Bream)
  - 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, including when patterns of incidents occur
  - liaises with the Local Authority and / or other relevant body
  - liaises with school network manager
  - receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
  - meets regularly with the Online Safety Governor (Lynda Townsend) to discuss current issues, review incident logs and filtering/monitoring logs
  - attends relevant meetings of Governors
  - reports regularly to Senior Leadership Team

3.5 The Network manager / School Business Manager

Pitmaston Primary school use Netbuilder as their Network Manager.

The network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents that they discover are logged (see appendix 5) and dealt with appropriately in line with this policy
- Users may only access the networks and devices through a properly enforced password protection policy

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the Online Safety Lead and DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school safeguarding policy
- Reporting any suspected misuse or problem to the Online Safety Lead and DSL

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Help and advice - Childnet International
- Parent resource sheet - Childnet International
- Support around the consensual and non-consensual sharing of nudes and semi-nudes (previously referred to as sexting) – internetmatters.org

Pitmaston 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.

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. They will be expected to agree to the terms on acceptable use before they are able to sign onto the network (appendix 3).

4. Educating pupils about online safety

As written in KCSiE 2024: It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. The education of pupils in online safety/computing is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum including through PHSE which includes aspects about online safety.

As it states in Keeping Children Safe in Education, the breadth of issues associated with online safety is considerable, but can be categorised into four main areas:

• content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

At Pitmaston Primary School, we have planned a curriculum that ensures the following:

- Specific online safety lessons are delivered once a month following a progressive theme across the school from Foundation Stage to year 6. (Following Project evolve and the 8 Areas of Learning; online reputation, cyber bullying, privacy and security, managing online information, self-image and identity, copyright, online relationships and health, well-being and lifestyle.)
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils build awareness of and 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.
- Pupils who have achieved lower than expected outcomes in any areas linked to online safety and pupils with language and communication barriers will receive pre-teaching of earlier year group lessons to overcome difficulties in accessing the lesson.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Complete lessons linked to Project Evolve ensuring full coverage of all 8 areas identified within this curriculum

  (this is not an exhaustive list)

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Complete lessons linked to Project Evolve ensuring full coverage of all 8 areas identified within this curriculum
- Identify a range of ways to report concerns about content and contact (this is not an exhaustive list)

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5. Educating parents about online safety

The school will raise parents' awareness of online safety concerns through PA connect/ Social Media, and in information via our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Online Safety Lead, Rachel Harber and/or the DSL.

6. Cyber-bullying

6.1 Definition

Cyberbullying (or online bullying) is bullying using technologies, particularly over the internet or via mobile and gaming networks to deliberately and repeatedly upset someone else. Cyberbullying can be an extension of face-to-face bullying, with technology providing an additional route to harass an individual or group. Cyberbullying can include: intimidation and threats, harassment and stalking, vilification/defamation, exclusion or peer rejection, impersonation, unauthorised publication of personal information or images and manipulation (Taken from Childnet.com)

~~Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour and relationships policy.)~~

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes, and where appropriate the issue will be addressed in assemblies as well as other planned opportunities such as Online Safety Week.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on online safety which includes cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

Pitmaston will (when appropriate) also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and relationships policy as well as following relevant guidance from the DfE. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, or there is reason to believe that a young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent, and will work with external services if it is deemed necessary to do so. This also applies to incidents relating to the sharing of consensual and non-consensual nudes and semi-nudes.

6.3 Examining electronic devices

If it is reported that a pupils has inappropriate material on an electronic device, it will be reported immediately to the DSL/DDSL in line with our safeguarding procedures. The DSL/DDSL will then decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE’s latest guidance on screening, searching and confiscation.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school (Please also refer to the Mobile Phone Policy)

While we fully acknowledge a parent’s right to allow their child to bring a mobile phone to school if they walk to and from school without adult supervision, Pitmaston Primary discourages pupils bringing mobile phones in year groups below Year 5 & 6. Phones are turned off and left securely with their class teacher on arrival into the school building. Children are not permitted to use them during the school day or during any extended before and or afterschool activity.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour and relationships policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their school device, they must seek advice from the network manager/business manager.

Work devices must be used solely for work activities and cannot be taken off site without written consent of the business manager/Headteacher.

10. How the school will respond to issues of misuse

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in our policies on behaviour and Internet Acceptable Use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. 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.

11. Training

All new staff members will receive training, as part of their induction, on the use of the school network including cyber-security and online safety including the risk of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, briefing minutes 7 minute updates and staff meetings).

The DSL and DDSL’s will undertake child protection and safeguarding training, which will include online safety, annually. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on cyber security and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The Online Safety Lead monitors behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Online Safety Lead and DSL. At every review, the policy will be shared with the governing body and staff

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour and relationships policy
- Staff disciplinary procedures
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Mobile Phone policy

Appendix 1: KS1 acceptable use agreement (pupils and parents/carers)

Pitmaston Primary School

AUP for Children in KS1

When I am using the computer I want to feel safe all the time.

I agree that I will:

- use the school ipads/computers to go on games or websites my teacher has told me to use.
- tell my teacher if anything on the internet makes me feel scared or worried
- talk to my teacher before using anything on the internet
- not share information about myself with people online (I will not tell them my name, address or anything about my home, family or pets)
- I will take care of the computer/tablets and other equipment
- I know that if I break the rules I might not be allowed to use a computer/tablet

I know that anything I do on a school computer/ipad will be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Name of Pupil .... Class ....

Pupil's Signature.. Date ....….........

Parent/ Guardian's Signature .... Date ....

Parents and carers can get advice and information on helping children stay safe on the internet on

www.thinkuknow.co.uk/parents

Appendix 1: EYFS acceptable use agreement (pupils)

Pitmaston Primary School

Acceptable Use Policy for Children in Early Years

When I am using the computer I want to feel safe all the time.

I agree that I will:

- only open computer games which my teacher has said are OK
- tell my teacher if anything on the internet makes me feel scared or worried
- I will take care of the computer/tablets and other equipment
- I know that if I break the rules I might not be allowed to use a computer/tablet
-

Name of Pupil .... Class ....

Parent/ Guardian’s Signature .... Date ....

CLICK CEOP
Internet Safety

Every web page has a CEOP button that can be used to log a concern.

Parents and carers can get advice and information on helping children stay safe on the internet on

www.thinkuknow.co.uk/parent

Appendix 2: KS2 acceptable use agreement (pupils)

Pitmaston Primary School

AUP for Children in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will

- Only use the school computers/ipads for activities my teacher tells me to complete on websites they have told me to use.
- always keep my passwords a secret
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- be polite and respectful when I communicate with others online
- not reply to any inappropriate message or anything that makes me feel uncomfortable
- not use my own mobile device (mobile, camera or USB memory stick) in school
- only give my mobile phone number to friends I know in real life and trust
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others

CEOP REPORT
ceop.police.uk

I am aware of the report and block buttons on social networking sites and know when to use them.

I know that anything I share online will be monitored.

I know the searches I complete and websites I visit are monitored by the school’s network.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Name of Pupil...   Class...............................

Pupil’s Signature..   Date................................

Parent/ Guardian’s Signature..   Date.............................

Parents and carers can get advice and information on helping children stay safe on the internet on www.thinkuknow.co.uk/parents

Appendix 3: Staff (and Volunteer) Acceptable Use Policy Agreement

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 network and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will 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 ICT 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. Where these images are published (e.g. on the school website, school social media) it will not be possible to identify by name, or other personal information, those who are featured without the permission of the parent or guardian.
- I will only use social networking sites in school in accordance with the school's policies.
- 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:

- When I use my mobile devices (mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), inappropriate or which 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 install or attempt to install programmes of any type on a device, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I 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 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 if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and or the Local Authority and in the event of illegal activities the involvement of the Police.

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

Staff / Volunteer Name: ………………………………………………………

Signed: …………………………………………

Date: ………………………………………………………

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Online Safety Incident Report Log

Pitmaston Primary School Online Safety Reporting Log

Date	Name of Pupil or staff Member	Male or Female	Room / Computer number	Incident	Action Taken
					What? By Whom?

Appendix 6: Online Safety Reporting Form

Online Safety - Record of Concern/Incident

Pupil Name: _______________________ Class: __________ Date:______

Reported by ________________________

Area of concern

Inappropriate gaming	Inappropriate viewing	Cyber bullying	Sharing of nude and semi nude images	Potential grooming
Nature of concern				
Actions taken / Outcome				
Reported to: Date and time: Signed:				

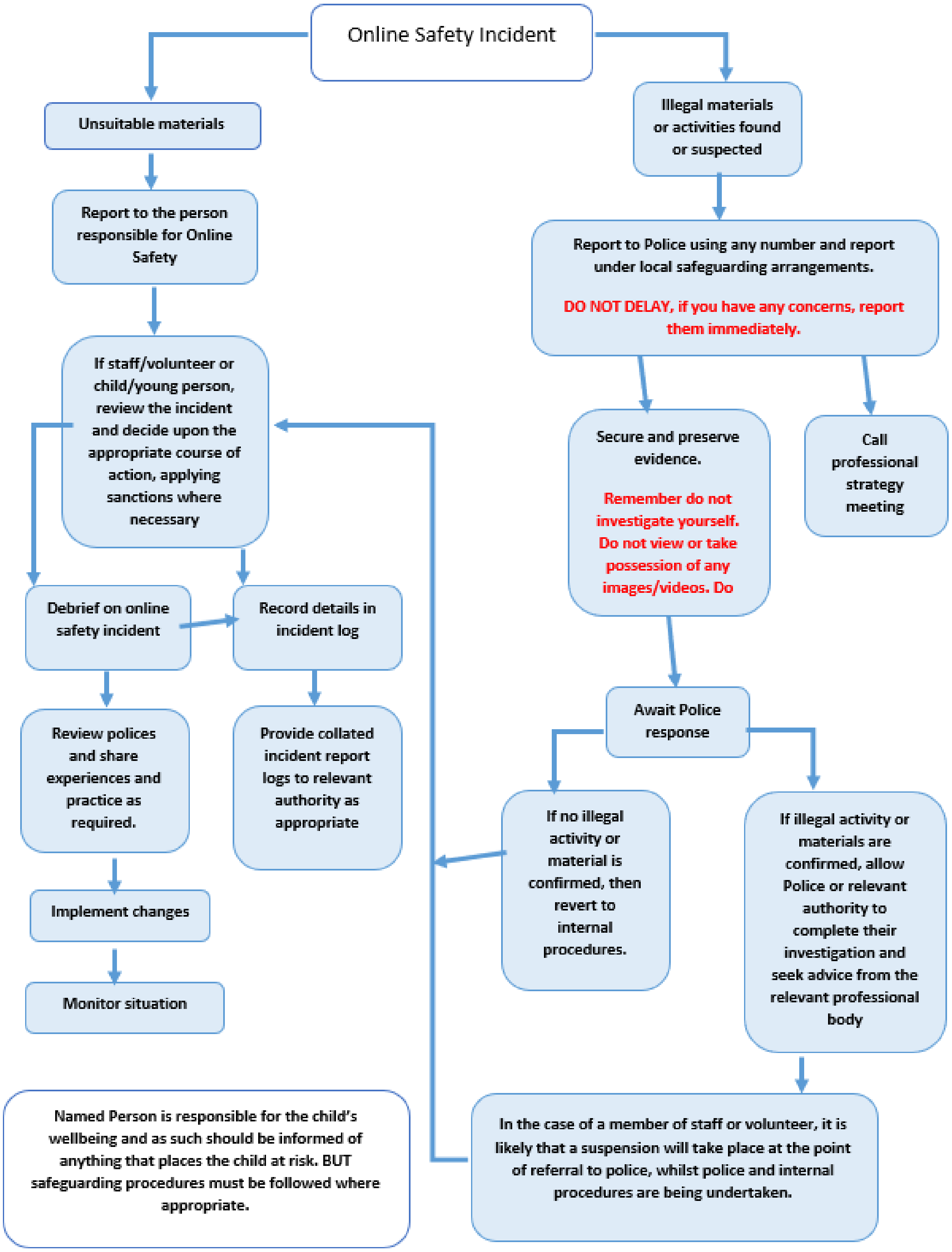
Appendix 7: Responding to Online Safety Incidents Flow Chart

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

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 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
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.
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.