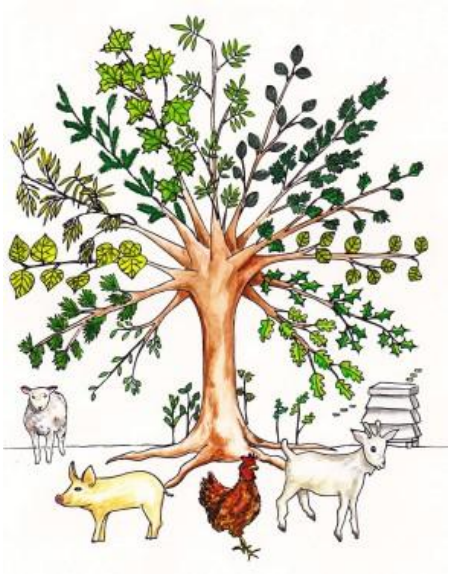
Edwalton Primary School



Online Safety Policy

including Prevent and statutory requirements for Sex and Relationship Education

Reviewed September 2026 (to include changes in KCSIE 2026)

Next review September 2027

Contents

1. Aims

2. Scope of policy

3. Legislation and guidance

4. Roles and responsibilities

5. Policy statements

6. Cyberbullying

7. Technical – infrastructure / equipment, filtering and monitoring

8. Pupils using mobile devices in school

9. Responding to incidents of misuse

10. Links to useful websites

Appendix 1: online safety training needs – self-audit for staff

Appendix 2: online safety incident report log

Staff (and Volunteer) Acceptable Use Policy Agreement

Pupil Acceptable Use Agreement KS1

Pupil Acceptable Use Agreement KS2

1. Aims

Our school aims to:

- 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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 8 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as 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, such as 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
- Misinformation – false or inaccurate information
- Disinformation – false information deliberately intended to mislead
- Conspiracy Theory – the belief that some secret, but influential organisation is responsible for an event or phenomenon.
- Use of AI – AI can be a useful tool to use, but pupils must also be aware that it can be used inappropriately or be used to mislead pupils.

2. Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers and visitors who have access to and are users of school ICT systems, both in and out of the school.

3. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE'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.

This policy complies with our funding agreement and articles of association.

4. Roles and responsibilities

Head teacher

Are responsible for ensuring that:

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

Designated safeguarding lead (DSL)

Are responsible for ensuring that:

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 2) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 1 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 board
- Undertaking annual risk assessments that consider and reflect the risks children face

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *school* Online Safety Policy and practices
- they understand their obligations under the Keeping Children Safe in Education statutory guidance
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problems to the Headteacher *or* SENCO for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- they recognise the warning signs of children at risk of radicalisation or extremism and report in line with Prevent Duty (1st July 2015)
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Following the correct procedures by contacting the IT lead if they need to bypass the monitoring systems for educational purposes.

Resources for teaching E-Safety

- National Online Safety
- Purple Mash
- KidSmart http://www.kidsmart.org.uk/
- BBC Stay safe http://www.bbc.co.uk/cbbc/help/web/staysafe
- Be internet awesome by Google
- Think U Know from NCA/CEOP https://www.thinkuknow.co.uk/
- Picture News

The IT lead

Are responsible for ensuring that:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 2) 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 behaviour policy

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. 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
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

5. Policy Statements

Education – Pupils

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 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. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited and also with guidance on relationships education, relationships and sex education (RSE) and health education.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should 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 should act as good role models in their use of digital technologies the internet and mobile devices

Pupils will be taught the following as part of our e-safety program:

How to evaluate what they see online - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

- Pupils will be asked to consider questions including:
    - is this website/URL/email fake? How can I tell?
    - what does this cookie do and what information am I sharing?
    - is this person who they say they are?
    - why does someone want me to see this?
    - why does someone want me to send this?

- why would someone want me to believe this?
- why does this person want my personal information?
- what's behind this post?
- is this too good to be true?
- is this fact or opinion?

How to recognise techniques used for persuasion – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

- Children will be supported to recognise:
  - online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
  - techniques that companies use to persuade people to buy something, 7 ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and criminal activities such as grooming.

Online behaviour – This will enable pupils to understand what acceptable and unacceptable online behaviour look like. We will teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. We will also teach pupils to recognise unacceptable behaviour in others.

- We will help pupils to recognise acceptable and unacceptable behaviour by:
  - looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
  - looking at how online emotions can be intensified resulting in mob mentality,(how people can be influenced by their peers to adopt certain behaviours on a largely emotional, rather than rational, basis)
  - teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and
  - considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

How to identify online risks – This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

We will help pupils to identify and manage risk by:

- Identifying and understanding the 4 Cs: contact, conduct, contact and commerce
- discussing the ways in which someone may put themselves at risk online,
- discussing risks posed by another person's online behaviour,

- discussing when risk taking can be positive and negative,
- discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e how past online behaviours could impact on their future, when applying for a place at university or a job for example,
- discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
- asking questions such as what might happen if I post something online? Who
- will see it? Who might they send it to?
- What are the four things you need to be careful about sharing online with others?

How and when to seek support – This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

We will help pupils by:

- helping them to identify who trusted adults are,
- looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This links to wider school policies and processes around reporting of Safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education); and
- helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.
- Helping them identify important information and how to keep it and them safe.
- Helping them to understand that they should seek advice before trying something new online or, to talk to a trusted adult should something make them feel sad, worried or confused.

Who to talk to should they need support – This will enable children to know who is available to support the children should they need it:

- **Childline** for free and confidential advice
- **UK Safer Internet Centre** to report and remove harmful online content
- **CEOP** for advice on making a report about online abuse

Children to be aware of online safety which can be classified into four areas of risk:

- **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 or 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.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference: https://www.gov.uk/government/publications/education-for-a-connected-world

Education & Training – Staff / Volunteers / governors

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 will be 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 should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- Participation in school / academy training / information sessions for staff or parents
- Staff to be trained to identify behaviour that causes concern that the child is at risk of radicalisation or extremism.

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Hetvi Parekh.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

6. Cyberbullying

Definition

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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.

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

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

The school 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 policy. 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7. Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT Co-ordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Filtering and monitoring will ensure that children are kept safe from terrorist and extremist material when accessing the internet in school in line with current guidance of the Prevent Duty (1st July 2015)

If inappropriate material is found on the device, it is up to DSL's (Charly Soulsby , Trish Gilbert, Alice Jackson and head teacher (Dan Graney) and Computing Lead (Luke Morledge) to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage. The school allows:

	School Devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes (locked away during the school day)*	*Yes (subject to acceptable use)*	*Yes*
Full network access	*Yes*	*Yes*	*No*	*No*	*No*
Internet only		*Yes*	*No*	*Yes*	*No*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

8. Artificial intelligence and emerging technologies

The school recognises that artificial intelligence (AI) and emerging technologies are becoming an increasingly common part of children's online experiences. While these technologies can provide valuable educational opportunities, they may also present safeguarding risks including:

- Exposure to inaccurate or misleading information,
- AI-generated content,
- manipulated images or videos,
- online scams, and
- inappropriate interactions through digital platforms.

The school will promote the safe, responsible and age-appropriate use of AI and emerging technologies by providing pupils with opportunities to develop critical thinking, digital literacy and online safety skills. Staff will receive appropriate training to understand potential risks and will respond promptly to any safeguarding concerns arising from the use of AI or other emerging technologies. Online safety education will help pupils to question, verify and evaluate online content and understand how to seek support if they encounter anything that causes concern.

9. Pupils using mobile devices in school

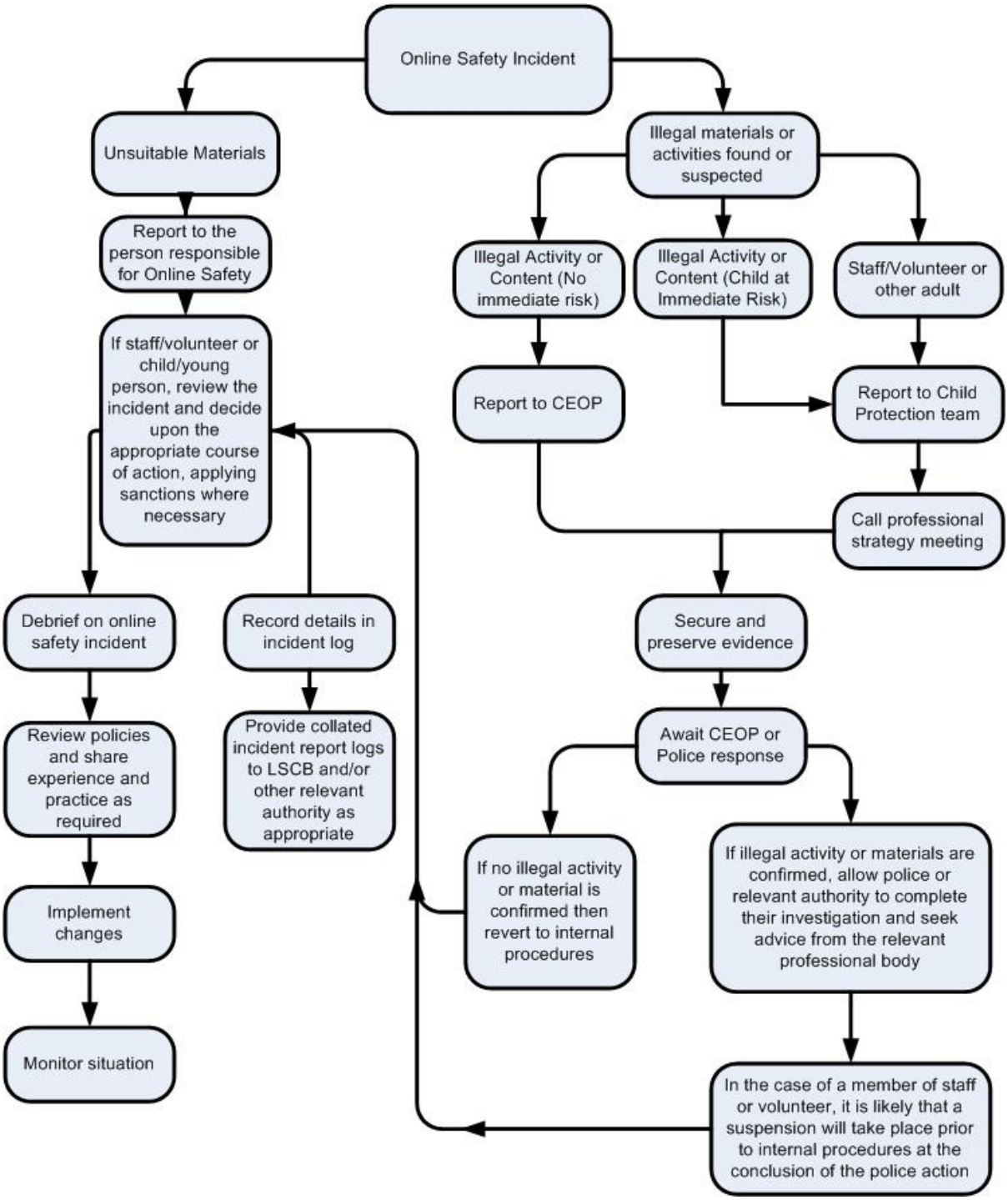
Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

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 policy, which may result in the confiscation of their device.

10. Responding to incidents of misuse – flow chart



10. Links to useful websites

UK Council for Child Internet Safety (UKCCIS);

Child Exploitation and Online Protection Centre (CEOP);

Think U Know website;

BBC Chat Guide;

Childline

UK Safer Internet Centre;

Childnet International

Grid Club and the Cyber Café

Cybermentors

Internet Watch Foundation

SWGfL (South West Grid for Learning)

E-Safety in Stoke Schools

Kidsmart

NSPCC

Internet Safety Zone

NCH – The Children's Charity

SCARF – Safety, Caring, Achievement, Resilience, Friendship - PSHE

Parents Protect

That's not cool

Digizen

Internet Matters

Vodafone Digital Parenting Guide – Keeping kids safe online

Appendices

Appendix 1: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer: Luke Morledge	**Date**: 05/09/24
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	Yes – DSL's and Computing Lead
Are you aware of the ways pupils can abuse their peers online?	Yes – cyberbullying, radicalisation, shaming
Do you know what you must do if a pupil approaches you with a concern or issue?	Yes – instantly share with the DSLs
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	Yes
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	Yes
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	Yes – we recently have been added to a new software called Senso Alerting which was installed by LEAD IT.
Do you understand your role and responsibilities in relation to filtering and monitoring?	Yes
Do you regularly change your password for accessing the school's ICT systems?	Yes – every year we are prompted to change them. We can do it more regularly if requested by DSLs or IT Lead.
Are you familiar with the school's approach to tackling cyber-bullying?	Yes
Are there any areas of online safety in which you would like training/further training?	No

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**
Nov-2023	Classroom – using laptops	A child had been searching on Google and had been entering inappropriate words which were unrelated to their lesson's learning.	Child was spoken to about their use of technology and how everything they do on a computer, in and out of school can be tracked back to them.	Tommy Brown TBrown

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 systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / 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. laptops, email, VLE etc.) out of school, and to the transfer of personal data 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 ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published it will not be possible to identify by name, or other personal information, those who are featured.
- 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 personal mobile devices 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 understand that I may not use personal electronic devices when children are present and I must never take or store images of children on a personal device.
- I will not use personal email addresses on the school / academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will 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) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that 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 safeors 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: .....

Pupil Acceptable Use Agreement KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computing equipment in school (this includes laptops and iPads).
- I will only use websites, applications (apps) and software that a teacher or suitable adult has told or allowed me to use.
- I will follow all instructions given to me by a teacher or responsible adult.
- I will take care of the computing equipment so that it is available for others to use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do.
- I will ask for help from a teacher or suitable adult if I think that there is something wrong or I have accessed something by mistake.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will treat everyone fairly and with respect when communicating with them online
- I understand that people I do not know are strangers on the internet and I must not share my own, or anybody else's, personal information (this includes names, date of birth, email, address, school name).
- I will keep all passwords safe and not share them with anyone else.
- I know that if I break the rules I may not be allowed to use the computer equipment and if necessary further action may be taken.

Pupil Acceptable Use Agreement KS2

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computing equipment in school (this includes laptops and iPads).
- I will only use websites, applications (apps) and software that a teacher or suitable adult has told or allowed me to use.
- I will follow all instructions given to me by a teacher or responsible adult.
- I will take care of the computing equipment so that it is available for others to use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do.
- I will ask for help from a teacher or suitable adult if I think that there is something wrong or I have accessed something by mistake.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will treat everyone fairly and with respect when communicating with them online and understand that cyberbullying is not acceptable.
- I understand that people I do not know are strangers on the internet and I must not share my own, or anybody else's, personal information (this includes names, date of birth, email, address, school name).
- I will keep all passwords safe and not share them with anyone else.
- I understand that the use of computers in school is digitally monitored and any attempts to access websites, software or applications will be reported.
- I understand that I must only download digital content that I have permission to use – this includes pictures and videos from websites.
- I know that if I break the rules I may not be allowed to use the computer equipment and if necessary further action may be taken.