Hunsley Primary

Online Safety Policy V3

This policy is applicable to Hunsley Primary
To be read with reference to the Trust and School suite of Safeguarding and Child Protection Policies and Procedures which are located on the school website and the Statement for the Safe Use of Multi Media in the Classroom and Beyond.

Important: This document can only be considered valid when viewed on the school website. If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online. **Name and Title of Author:**	Julie Boyes Assistant Head
Name of Responsible Committee/Individual:	Hunsley Primary Local Governing Body
Version:	3
Implementation Date:	Summer Term 2026
Review Date:	Summer Term 2028
Target Audience:	All Staff, Parents, Pupils, Community Users, Key Stakeholders

Introduction

The use of technology continues to be an important component of safeguarding young people. Technology, whilst providing many opportunities for learning also provides a platform that can facilitate harm. 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 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. Keeping Children Safe in Education categorises online safety into four broad areas:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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 (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and ~~or~~ online bullying.
- **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/).

It is with these four categories in mind that this policy outlines the roles, responsibilities and procedures for ensuring online safety.

Aims

This policy aims to set out the school's position in how it will strive to provide a safe environment for all of the school community whilst using ICT within the school, and how it will also strive to ensure that its members also use ICT, including their own personal devices, in a safe and responsible manner whilst outside of the school grounds.

This policy will detail the individual responsibilities of each of the key people in the school who have a role to play in fulfilling this policy and its related procedures.

This policy applies to all staff, children, governors and parents of the school community. It should be read in conjunction with the supporting policies and related information that is detailed below.

Hunsley Primary believes that ICT can and should be used to enrich the education of all children. ICT also provides the staff of the school with a great many tools to help them play their part in providing the children of the school their education. Whilst the school sees the benefits of using this technology, it is also aware of the potential risks that the internet, ICT and related technology can pose. The school believes that online safety is the responsibility of the whole school community, and that all members of that community have their own part to play in ensuring that everyone can gain from the benefits that the internet and ICT afford to teaching and learning, whilst remaining safe.

Social Networking is becoming an increasingly popular tool within our environment to support learning, encourage creative and appropriate use of the internet and to publish and share content. These

technologies need to be used in a safe and responsible way, and appropriate online behaviour encouraged. We also expect staff to maintain a professional level of conduct in their use of these types of technologies.

Inclusion, Equality and Diversity

Hunsley Primary and the Education Alliance are committed to:

- Promoting equality and diversity in its policies, procedures and guidelines
- Delivering high quality teaching and services that meet the diverse needs of its student population and its workforce, ensuring that no individual or group is disadvantaged.

Vision, Values and Ethos

Vision: Our Commitment

Hunsley Primary is committed to being an innovative, stimulating, forward-thinking free school that makes the most of its freedoms to impact positively on pupils' lives in the community and provide opportunities for all its children to make outstanding progress. Hunsley Primary children are capable, confident and creative thinkers and motivated, resilient, problem-solving learners.

Values: Our Children

At Hunsley Primary, we believe that every child is an individual, ready, able and eager to learn, and as such a member of the team. We are a fully inclusive school, and we view every child as unique; we believe that all learning activities should be personalised and challenging to meet all pupils' needs and that every child should receive the care, guidance, nurture and robust support they need to overcome disadvantage or barriers to learning. It is our prime aim that all children make their best progress in an enabling learning environment, in the presence of their peers and the security of positive relationships with those around them. Our highly trained expert classroom practitioners, from teachers, TAs, volunteers to associate Trust staff, ensure that all children have the chance to work, discuss and learn with professionals who are passionate about education.

By ensuring our children become responsible for directing, sustaining and reviewing their own learning, taking responsibility for critiquing their own and each other's work and for setting ambitious challenges, we aim to embed an understanding of the importance of refining work to its best point so that children feel a sense of high achievement because of the feedback they receive.

By maximising the benefits of our close relationship with South Hunsley School and Sixth Form College and its subject specialists, we aim to secure a continuum of learning and a depth of conceptual understanding necessary for excellent progress in all curriculum areas, leading to the highest achievement at Key Stage 2, GCSE and A Level and, in due course, access to the most aspirational HE institutions, courses or professions for all children.

Ethos: Our Teaching and Learning Rationale

Engagement, Enjoyment, Discovery, Reflection, Achievement

Our aim is to deliver teaching and learning which meets the needs of every single pupil in school, basing our planning on rigorous assessment and observation, mapping out challenging, supportive next steps. We plan our curriculum activities and our personalised teaching and learning approach to match the following rationale:

- Flexible, personalised timeframes for learning, based on excellent pupil-centred teaching – teachers highly conversant in the complexities and specialisms of their practice.

- Real learning themes and deep-thinking investigations, which prepare our pupils for 21st Century living and engage them in learning with enjoyment and passion.
- Inspirational and challenging learning activities, which have the principles of scientific enquiry and investigation ('working scientifically') at their core, generating a lifelong love of learning, enquiry and discovery and a systematic means of approaching challenging and new tasks.
- A union of partnerships with cross-phase, multi-agency and multi-disciplinary expertise for planning, delivery, monitoring and review, to ensure each child has every opportunity to build successfully on their learning from 4 to 19, removing barriers to engagement and development.
- Pupil resilience, independence, confidence, and readiness to meet the rigors of education, through to university and beyond, and the demands of living and working in a rapidly changing technological world.
- Innovative, immersive, and inclusive learning resources, combining the best of expert input, outdoor, firsthand, experiential learning, and digital interfaces, to give pupils every opportunity to aspire to their full potential.

1. Risks & Responsibilities

Risks of ICT use and the Internet

The school has identified the following risks that ICT and the internet can pose to its community: [1]

- Obsessive use of the internet and ICT
- Exposure to age-inappropriate materials
- Inappropriate or illegal behaviour
- Consensual and non-consensual sharing of inappropriate content and images
- Physical danger or sexual abuse
- Being subjected to harmful online interaction with other users
- Inappropriate or illegal behaviour by school staff
- Actions that bring the school into disrepute
- Online grooming or child exploitation
- Use of AI

Creating a Safe ICT Learning Environment

The school believes that the best way to provide a safe ICT learning environment is a triple-fold matter:

1. Create an infrastructure of **whole-school awareness**, **designated responsibilities**, **policies and procedures**. This is achieved by:
    - Raising awareness of the risks of ever-changing technology that is both emerging and already embedded in the school community.
    - Ensuring that the Online Safety policy and education programme adapt to meet these new and emerging technologies and is reviewed as incidents occur.
    - Establishing a clear understanding of the responsibilities of all of those involved with the education of children, with regards to Online Safety.

[1] This list is by no means exhaustive but means to highlight some of the main areas of risk that the school has identified.

- Ensuring that the school's policies and procedures are effective and kept up to date and make clear to all members of the school community what is acceptable when using ICT and the internet.

2. Make use of **effective technological tools** to ensure the safe use of the internet and school ICT systems. These include:
    - Firewall protection to the school's network.
    - Virus protection of all relevant IT equipment connected to the school's network.
    - Filtering, logging and content control of the school's internet connection.
    - Monitoring systems.
3. Develop an **Online Safety education programme** for the whole school. This will consist of:
    - An on-going education programme for the children at the school, so that they are given the tools to formulate and develop their own parameters of acceptable behaviour and take these with them when they leave the school.
    - Continued Professional Development for staff to ensure that they are equipped to support the children at the school and are also fully aware of their responsibilities in using ICT, both in and out of the school.
    - An on-going education programme for parents, carers and the wider community so that they have the knowledge and tools available to support the actions of the school in these matters.
    - Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.
    - Teaching why certain behaviour on the Internet can pose an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practices such as grooming can develop.
    - Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.
    - Explore the positives and negatives of using AI

Headteacher's Responsibilities

1. To take ultimate responsibility for online safety whilst delegating the day-to-day responsibility to an Online Safety Coordinator (OSC) – NB - this might be a role the Headteacher also takes up or the DSL.
2. To ensure that the OSC DSL is given enough time, support and authority to carry out their remit.
3. To ensure that the local governing body is kept informed of the issues and policies.
4. To ensure that the appropriate funding is available to support the technological infrastructure and CPD training for the online safety programme.

Governing Body's Responsibilities

1. To ensure the Designated Safeguarding Governor considers online safety as a part of the regular review of child protection and safeguarding.

2. To support the Headteacher and / or OSC DSL to ensure that the correct policies and procedures are in place, and that the funding required to achieve these policies and procedures is available.
3. To help in the promotion of online safety to parents.

Designated Safeguarding Lead's Responsibilities

1. To develop and review the appropriate online safety policies and procedures.
2. To develop management protocols so that any incidents are responded to in a consistent and appropriate manner.
3. To maintain a log of all online safety incidents that occur in the school.
4. To recommend reviews of technological solutions, procedures and policies based upon analysis of logs and emerging trends.
5. To seek professional development on the safety issues relating to the use of the internet and related technologies, and how these relate to young people.
6. To liaise with the OSC, Headteacher, Trust IT team and DSG on specific incidents of misuse.
7. Take a proactive role in the online safety education of the school's children.
8. Develop systems and procedures for supporting and referring children identified as victims or perpetrators of online safety incidents.
9. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.
10. To carry out an annual review of the school approach to online safety, supported by an annual risk assessment that considers and reflects the risks our children face.

IT Support Responsibilities

1. To perform regular audits and checks of the school's networked systems to look for signs of misuse or inappropriate files. Any such findings would need to be reported to the OSC, Headteacher and Police if necessary.
2. Review the technological systems upon any discovery or breach of the Trust Acceptable Use Policy (AUP), to ensure that the same breach does not happen again.
3. Liaise with the school DSL if any breach can be traced back to an individual child.
4. Liaise with the OSC DSL and Headteacher if any breach can be traced back to an individual member of staff.
5. Provide the technological infrastructure to support the online safety policies and procedures.
6. Report any network breaches of the Trust Acceptable Use Policy or Online Safety Policy to the OSC.
7. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Online Safety Coordinator's Computing Curriculum Team Responsibilities

1. To work with the appropriate members of staff to develop a staff CPD programme to cover all areas of online safety inside and outside of the school environment.
2. To work with the appropriate members of staff to develop an online safety education programme for the children.
3. To work with the appropriate members of staff to develop a parental awareness programme for online safety at home.
4. To meet with the Designated Safeguarding Lead regularly to discuss online safety and progress.
5. To liaise with any outside agencies as appropriate.
6. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Special Educational Needs Coordinator's Responsibilities

1. To develop and maintain a knowledge of online safety issues, with regard as to how they may affect children and young people with additional educational needs.
2. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Classroom Teachers', Teaching Assistants' and Site Staff Responsibilities

1. To develop and maintain a knowledge of online safety issues, regarding how they might affect children and young people.
2. To implement school online safety policies through effective classroom practice.
3. Understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of safeguarding training. For example, to monitor what's on pupils' screens. Report safeguarding and technical concerns, such as if:
    - They witness or suspect unsuitable material has been accessed
    - They can access unsuitable material
    - They are teaching topics that could create unusual activity on the filtering logs
    - There is failure in the software or abuse of the system
    - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
    - They notice abbreviations or misspellings that allow access to restricted material
4. To ensure any incidents of ICT misuse are reported through the correct channels.
5. To ensure that the necessary support is provided to pupils who experience problems when using the internet, and that issues are correctly reported to the OSC Computing Team/DSL.
6. To plan classroom use of ICT facilities so that online safety is not compromised.
7. To teach and remind the children about the school Safe APPS before using any online technology. (see Appendix 2)
8. To maintain an appropriate level of professional conduct in their own internet use, both within and outside the school.

Children's Responsibilities

1. To uphold all school online safety and ICT policies, including following Safe APPS (see Appendix 2)
2. To report any misuse of ICT within the school to a member of staff.
3. To seek help or advice from a teacher or trusted adult if they, or another child experience problems online.
4. To communicate with their parents or carers about online safety issues and to uphold any rules regarding online safety that may exist in the home.

Parents' and Carers' Responsibilities

1. To help and support the school in promoting online safety
2. To discuss online safety concerns with children and to show an interest in how they use technology.
3. To take responsibility for learning about new technologies and the risks they could pose.
4. To model safe and responsible behaviour in their own use of the internet.
5. To discuss any concerns, they may have about their children's use of the internet and technology with the school.

2. Procedures & Implementation

The school, through the Online Safety Coordinator DSL, will ensure that all staff are aware of the policies and procedures being implemented to meet the Online Safety remit. There will be information available to all staff about the technologies that are already in use at the school as well as new and emerging technologies that they may come across in their professional practice. All staff will be given the opportunity to feedback into the school's online safety discussions, be given clear guidance to what the procedures are and know who they should speak to regarding any issues.

Online safety will form a part of the Child Protection Induction for new staff starters and direct them towards the existing policies, procedures, resources and courses of action.

Children

The pupils at the school will be made aware that there is a whole school approach to online safety and their roles and responsibilities within this e-Safe environment will be made clear to them. Children will be invited to participate in the future planning and discussions regarding online safety and their opinions will be regularly gauged as to the effectiveness of the provision.

Parents and Carers

The parents and carers of the school will be made aware of policies and procedures and how they can help in ensuring that Hunsley Primary is an e-Safe school. We will ensure that parents and carers can access information regarding the risks of new technologies, but also how they can ensure these technologies are being used safely.

Parental workshops will be delivered to give parents the opportunity to understand online safety topics and new risks children are exposed to.

Firewall

The school has a perimeter firewall, which is supplied by Smoothwall. This physical hardware device sits at the edge of the network and allows only specific traffic in and out of the network. All intrusion attempts from both sides of the network can be logged and analysed for security audits.

The responsibility lies with the IT support staff and the DSL for ensuring that the firewall is correctly configured and that intrusion logs are regularly checked.

Monitoring and Filtering Systems

Filtering is preventative – protects users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

Monitoring is reactive – monitors what users are doing on devices. Effective monitoring is an important part of providing a safe environment for students and staff.

Our Monitoring and filtering system is SMOOTHWALL. This is real time, human moderated monitoring that alerts designated staff to students suspected of becoming vulnerable (24/7, 365 days a year). It monitors all school devices for concerns about; bullying, offensive use, oversharing, sexual content terrorism/extremism, vulnerability, grooming, general risk and violence.

Where incidents raise concern regarding a child's welfare they will be also recorded on our online Child Protection Monitoring System CPOMS where a pattern of concern can be identified if appropriate.

Currently, school-owned iPads are filtered through the web proxy with the most restrictive policy applied.

Online Safety Education

All children at the school will receive an on-going online safety education programme and will understand and use the school Safe APPS.

This programme will inform the children of the issues and potential risks of using the internet and emerging technologies. It will also equip them with the knowledge to ensure they are adequately protected and informed when in these environments as new technology is adopted. They will be given the information required to know who they can talk to and what their rights are if they do experience issues whilst using the internet.

The School's PSHE curriculum is under constant review to include emerging trends in children's online use and to address new uses as they arise.

The school will follow the Safer Internet Day programme and deliver those resources through PSHE and Assembly. Teachers will be informed about the content being delivered, and asked to discuss the content

after the assembly is given so that pupils have an opportunity to raise any concerns or issues from this information.

The PSHE and Talk Time Jigsaw Personal Development curriculum will be regularly reviewed to ensure that it has appropriate and relevant online safety content incorporated into its programme.

The SENCO will work with the OSC DSL and Computing Curriculum Team to ensure that there are accessible and adequate resources available for SEND pupils of the school to access the same online safety education as the rest of the school.

Use of AI

As a Trust we are developing our systems regarding the use of AI. The children will be taught the pros and cons of AI during their online safety and computing lessons. All TEAL staff are expected to watch the training video on our 'Principles of Using AI before using AI tools for work purposes/at work'.

The 'approved and prohibited' list mentioned in the training can be found at the link below. This is a live document, with updates also being shared via school bulletins. Approved Uses of AI in TEAL.docx

Responding to a concern

Appendix 1 outlines the process regarding concerns being raised relating to online safety.

As a school, we proactively work to ensure the safety of our children both in-school and online. We do not have the capacity to police all online activity outside of school, however where actions of a child online go against the school's Behaviour Policy, we will address these concerns directly.

Where actions taken by pupils online pose a risk to them or others, they will be dealt with in line with our Child Protection Procedure, conducting appropriate risk assessments and ensuring minimal disruption to any victim, where appropriate.

Consistent Approach

The OSC DSL will ensure there is a commonality of approach in responding to online safety incidents and that the correct reaction and procedure is followed by all staff when dealing with an online safety issue.

School Social Media Accounts

The school hosts social media accounts (Twitter and Facebook) which are maintained only by authorised staff.

Whilst all social media is different, and constantly evolving there are some key expectations for colleagues using social media in school, which are as follows:

- All social media must be set up to ensure that that there can be no private communication or Direct Messaging between the account and the accounts of pupils.
- Passwords should not be shared between colleagues and one colleague should take overall responsibility for the account and its content.
- Users should follow the expectations and responsibilities of colleagues outlined above.

As stated above, social media is constantly changing and as such advice should be sought from the OSC where appropriate.

Supporting Policies and Related Information

Hunsley Primary/Education Alliance supporting policies:

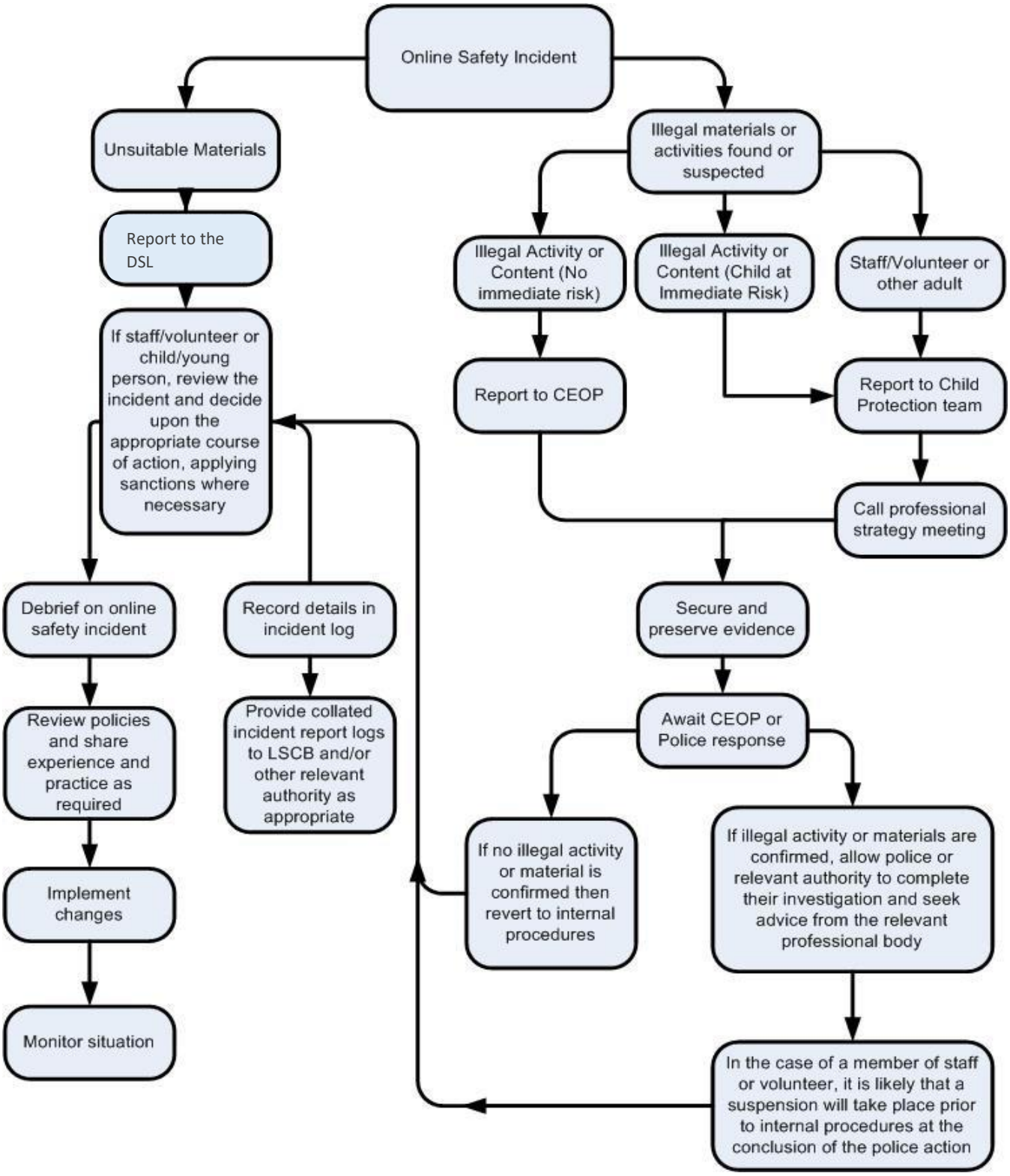
- Child Protection Policy & Procedure and suite of safeguarding policies (e.g. Educational Visits)
- Trust Expectations and Code of Conduct for Staff
- Prevent Policy
- Behaviour and Sanctions Policy
- Trust / Schol Acceptable Use Policy
- Statement for the Safe Use of Multimedia in the Classroom and Beyond
- Expectations of Use: School IT Equipment
- Hunsley Primary SafeAPPS (Appendix 2)

Procedure for Policy Implementation

The procedural document for this policy is attached as an appendix.

- Appendix 1 – Online Safety Incident Reporting Flowchart

Appendix 1 - Responding to incidents of misuse (Flow Chart)



Appendix 2 – School SafeAPPS posters


HUNSLEY PRIMARY
STAYING SAFE ONLINE
HUNSLEY PRIMARY
HUNSLEY PRIMARY Safe APPS
A
P
P
S
Ask Always ask before you use a device and use it when an Adult is nearby. Don't have too much screentime!
Personal Information This is Private and shouldn't be shared with people you don't know.
Don't share your name, address, school, phone number or places you go.
Photos These are for your family and friends. Never send a photo of yourself without checking with your Parents. If someone asks for a photo online, tell your grown-up.
Say Something If something doesn't seem right, don't switch off - Shout out! We check what you look for online in school to keep you safe - let your grown-up decide what to do.


HUNSLEY PRIMARY
SAFE Apps KS2 – KeepingSafe2
HUNSLEY PRIMARY
Stop
• Stop and think before you share! Your photos, personal information and words will no longer be under your control once you have published them. Don't use other people's ideas, images or words without their permission.
Alert
• Are you protecting your passwords? Be alert about security at all times. Change your passwords regularly and never share them.
Fake
• Is it fake or is it real? News, views and images can all be fake and we need to take time to question it. Don't believe everything you see on screen! Think before you repeat it or try to copy it: is it the truth? Is it real?
Engage
• Are you an informed Internet user? If something worries you, don't ignore it: talk about it! Your teachers monitor what you search for and see online, and our filters keep you safe. Stay engaged: your online safety matters.