ONLINE SAFETY POLICY 2023/2025

Hartlebury Church of England (Voluntary Controlled) Primary School

Through love, we recognise everyone

as a **unique** child known to God.

We will walk with you on

your **journey** to reach your

full **potential**.

SB2023/2024 - VERSION 1 – 29.09.2023

Next review date: September 2025

Hartlebury Church of England (Voluntary Controlled) Primary School

Contents Page

Hartlebury Church of England (Voluntary Controlled) Primary School

ONLINE SAFETY POLICY

Aims of this Policy

Hartlebury Church of England Primary understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. This policy applies to all devices with the capacity to connect to the internet and transfer data. This includes internet-connected toys, tablets, smart TVs and watches, phones, laptops and computers.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff. All staff are trained annually in safeguarding children including the online safety element and have read and are aware of where to find Keeping Children Safe in Education 2022, the Department for Education's statutory safeguarding guidance.

At Hartlebury Church of England (VC) Primary we are committed to ensuring that:

- children and young people should never experience abuse of any kind.
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

(See also Appendix 2 – Incident Workflow)

The Law

Our Online Safety Policy has been written by the school, using advice from and government guidance. The Policy is part of the School Improvement Plan and related to other policies including
Child Protection and Safeguarding Policy, and Anti-Harassment and Bullying Policy.

Summaries of the key legislation and guidance are available at:

- Online abuse: https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- Bullying: https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- Child protection: https://learning.nspcc.org.uk/child-protection-system/england

Data Protection Policies

As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at: www.education.gov.uk/schools.

Roles and Responsibilities

The Executive Headteacher and the Head of School, alongside the online safety lead will:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored.
- Ensure staff training in online safety is provided and updated annually as part of safeguarding training.
- Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites.
- Ensure that all incidents of cyberbullying are investigated by the Head of School/DSL and reported to the Executive Headteacher.
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material.

The Head of School/DSL (Sophie Bartlett) is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND (special educational needs) face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO (Special Educational Needs Co-ordinator - Sophie Bartlett) and Computing Lead (Rebekah Salter).
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.
- Working with the Severn Academies Education Trust (SAET) ICT technicians, Joshua Bissell and Callum Caskey, to conduct half-termly light-touch reviews of this policy.
- Working with the Executive Headteacher and governing board to update this policy on an **annual** basis.

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely.
- Deliver a broad and balanced curriculum informing children how to safeguard themselves online.
- Monitor and supervise pupils' internet usage and use of other IT resources.
- Adhere to the Acceptable Use Agreement **(Appendix 1).**

- Engage in online safety training.
- Only download attachments/material onto the school system if they are from a trusted source.
- When capturing images, videos or sound clips of children, only use school cameras or recording devices ensuring all images are stored in a protected location i.e. password protected cloud storage.

It is essential that pupils, parents/carers, governors and the public at large have confidence in the school's decisions and services.

The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the SAET are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Online Safety training for Staff

The Head of School/DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-Harassment and Bullying Policy, the Behaviour Management Policy and the Child Protection and Safeguarding Policy.

Online Safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSHE (SCARF)
- PSHE/Citizenship
- Computing

The school will actively teach online safety at an age-appropriate level. The school follows a scheme of work (SCARF) for each year group covering: what should and shouldn't be shared online, password control and cyber bullying among other topics. Online safety will also be embedded throughout learning whenever children are using ICT in other lessons.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online.
- How to recognise techniques used for persuasion.
- What healthy and respectful relationships, including friendships, look like.
- Body confidence and self-esteem.
- Acceptable and unacceptable online behaviour.
- How to identify online risks.
- How and when to seek support.
- How to identify when something is deliberately deceitful or harmful.
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate.

The online risks pupils may face online are always considered when developing the curriculum. The Head of School/DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND (special educational needs) and LAC (looked after children).

Relevant members of staff, e.g. the SENDCO (Sophie Bartlett) and designated teacher for LAC (Rebekah Salter), work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Executive Headteacher and the Head of School/DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and Head of School/DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The Head of School/DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Notebooks
- Tablets
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Governors will:

- Ensure that this policy is effective and complies with relevant laws and statutory guidance.
- Ensure the DSL's remit covers online safety.
- Review this policy on an annual basis.
- Ensure their own knowledge of online safety issues is up-to-date.
- Ensure all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensure that there are appropriate filtering and monitoring systems in place.
- Ensure that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

Monitoring safe and secure systems

Internet access is regulated by a SAET-supplied filtered broadband connection (Smoothwall) which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords. If personal data has to be saved to other media, e.g. data sticks or CDs, it is to be encrypted or strong password protected. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times. Staff complete online Cyber Security Awareness training annually.

Safe use of the Internet and Web Filtering

- All staff and pupils will have access to the internet through the school's network.
- All staff, volunteers who have use of the school's IT equipment, must read and accept the Staff Acceptable Use Agreement each time they log onto a device in school.
- All children must read and accept the Acceptable Use Policy each time they log onto a device in school.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Executive Headteacher or Head of School, to pass to the SAET IT network manager (Joshua Bissell).
- If an adult finds a site that they consider unsuitable they should report it to the Executive Headteacher or Head of School/DSL.

The use of Email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails. All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email.

The School Website and Social Media

- The school website complies with statutory DFE requirements.
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted online Social Networking, Social Media and Personal Publishing (blogging).

Personal mobile phones and other mobile devices

- All mobile phone and hand-held device use by staff is prohibited in the Early Years Unit and areas which should be considered most vulnerable: toilets and changing areas, including where children change for swimming.
- All staff have access to lockers in the staffroom in which they should keep their personal mobile phone devices. Personal phone use during working hours is strongly discouraged. If access to personal mobile phones is required for 3CX calls or as a multi-factor authentication code generator to log into the CPOMS safeguarding platform, this should be done in the school offices or in the Rose Office.
- Staff needing to make calls or answer messages on their personal mobile phones or hand-held devices, may do so only in the school offices, Rose Office or in the staffroom.
- Children are prohibited from using personal mobile phones and hand-held devices in school. Children who are walking home from school may bring personal mobile phone devices to school but these must be handed into teaching staff at the start of the day for secure storage and returned at the end of the day. Teaching staff will note the owner and condition of each phone stored.
- School reserves the right to search the content of any mobile or hand-held device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring at the direction of the Executive Headteacher or Head of School.
- Staff are not permitted to use their own mobile phones or hand-held devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- Staff, governors and visitors who access the internet through the school's Wi-Fi network are made aware through their induction process that the data on their phones or devices will be monitored by the school's SAET-supplied filtered broadband connection (Smoothwall). Antivirus software has been installed on all computers and is to be maintained and updated regularly. Notifications of blocks to unsuitable websites made by Smoothwall will be received by the DSL and will be actioned as appropriate.

Managing online safety

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

The Head of School/DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

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

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

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The Head of School/DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the Head of School/DSL will balance the victim's wishes against their duty to protect the victim and other young people. The Head of School/DSL and other appropriate staff members will meet with the victim's parents/carers to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the Head of School/DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the Executive Headteacher who decides on the best course of action in line with the relevant policies.

If the concern is about the Executive Headteacher, it is reported to the Chair of Governors, Carolyn Gumbley. Referrals to the Local Authority Designated Officer (LADO) will be made as appropriate and by either the Head of School/DSL, Executive Headteacher or Chair of Governors.

The LADO is responsible for managing allegations against adults who work with children. This involves working with Police, Children's Social Care, employers and other involved professionals. The LADO does not conduct investigations directly, but rather oversees and directs them to ensure thoroughness, timeliness and fairness.

Concerns regarding a pupil's online behaviour are reported to the Head of School/DSL, who investigates concerns with relevant staff members, e.g. the Executive Headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Management Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Executive Headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves.

The Head of School/DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy. All online safety incidents and the school's response are recorded by the Head of School/DSL on CPOMS, the school.

Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook.
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse.
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

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

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

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

- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment.

The school will respond to these incidents in line with the appropriate policies.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding Policy.

Management of online safety incidents

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents take place and contribute to developments in policy and practice in online safety within the school;
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities.

Working in Partnership with Parents

Parents' attention will be drawn to the online safety policy and its implementation through the school newsletters, information evenings and on the school's website.

Protecting School Staff

In order to protect school staff, we require that parents/carers do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will act if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

The Education and Inspections Act 2006 empowers the Executive Headteacher and Head of School/DSL to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's Acceptable Use Policy.

Related policies and procedures

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019.
- The UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- DfE (2021) Harmful Online Challenges and Online Hoaxes.
- DfE (2023) Keeping Children Safe in Education 2023.
- DfE (2019) Teaching Online Safety in School.
- DfE (2018) Searching, Screening and Confiscation'.
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) Sharing nudes and semi-nudes: advice for education settings working with children and young people.
- UK Council for Child Internet Safety (2020) Education for a Connected World – 2020 edition.
- National Cyber Security Centre (2018) Small Business Guide: Cyber Security.

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

- Acceptable Use Policy
- Anti-Harassment and Bullying Policy
- Behaviour Management Policy
- Child Protection and Safeguarding Policy
- Confidential Reporting (Whistleblowing) Policy
- Keeping Children Safe in Education 2023
- Preventing Extremism and Radicalisation Policy

Appendix 1

SEVERN ACADEMIES
Educational Trust

SAET Acceptable User Policy

To qualify for Network, Internet and e-mail access, students and staff must read, and agree to this policy.

The Severn Academies Educational Trust strongly believes in the educational value of such electronic services and recognises their potential to support the curriculum. Every effort will be made to provide quality experiences for students and teachers using this information service. Inappropriate and/or illegal interaction with any information service is strictly prohibited.

If British decency laws are breached or the Computer Misuse Act 1990 is breached then a user is likely to have the matter referred to other authorities including the police. The Computer Misuse Act 1990 identifies three specific offences:

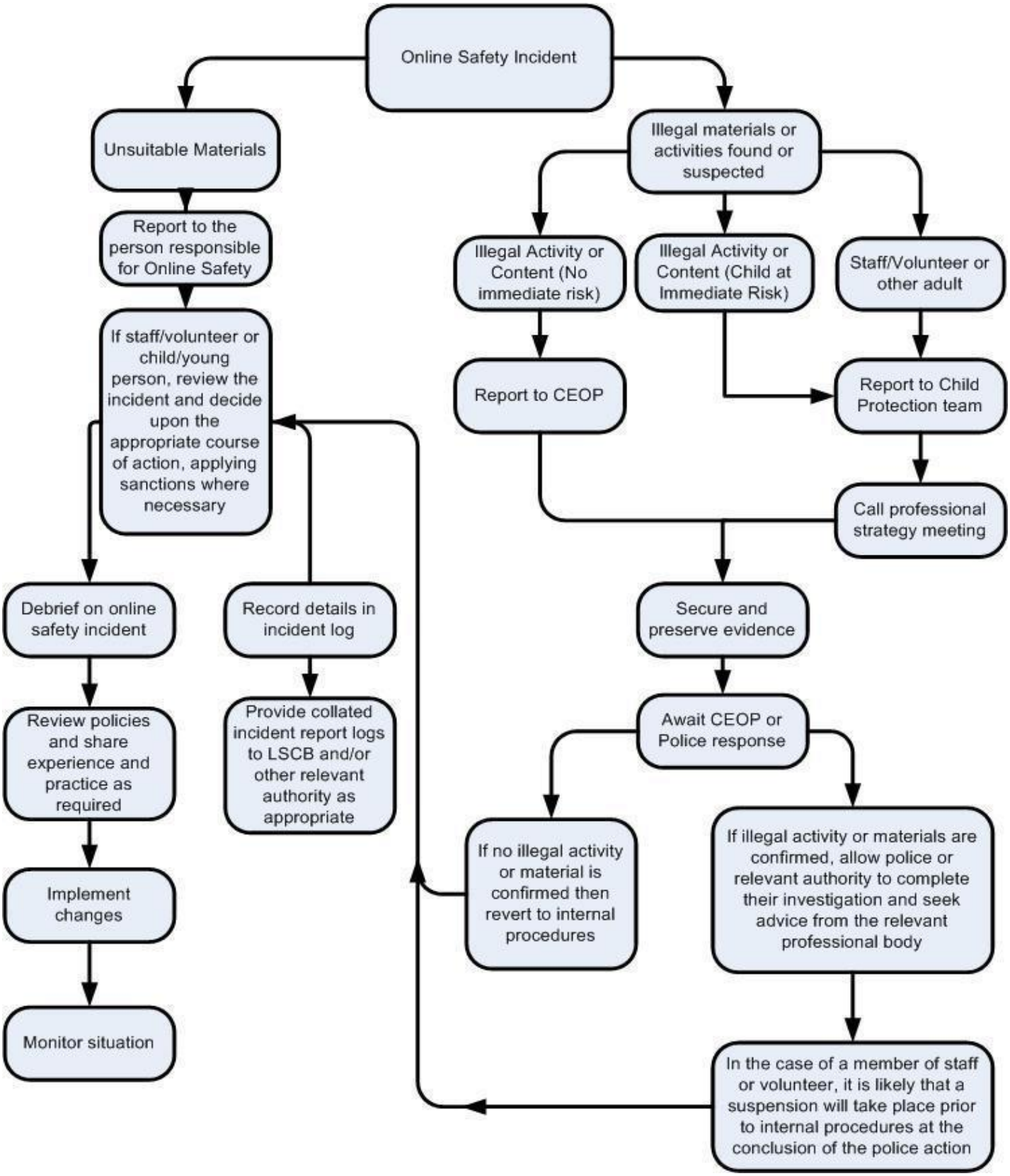
- Unauthorised access to computer material (that is, a program or data).
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
- Unauthorised modification of computer material.

Please read this agreement carefully, only once it has been agreed to will access to the computer system be permitted. Listed below are the provisions of this agreement. If any student or staff memberviolates these provisions, access to the Network, Internet and e-mail will be denied and you will be subject to disciplinary action.

Terms and Conditions of This Agreement:

1. No communications devices, whether school provided or personally owned, may be used for bullying or harassment of others in any form.
2. No applications or services accessed by users may be used to bring the trust, your school or it's members into disrepute (this includes social media).
3. All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
4. All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended.
5. All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.
6. All users must take responsibility for reading and upholding the standards laid out in this and all related polices.

Appendix 2


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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action