Haberdashers' West Midlands Academy Trust

Haberdashers' Abraham Darby

Online Safety Policy

2026-2027

ONLINE SAFETY POLICY	
Named Responsibility of Policy	Mrs C J Price Senior Vice Principal – Pastoral Deputy Designated Safeguarding Lead and Online safety lead
Date of Policy	September 2026
Date Approved by PSW Committee	20th October 2026
Date of Next Review	September 2027
Governor Accountability	Pupil and Staff Welfare Committee
This policy will be readily accessible to parents/carers, pupils, staff, visitors, and members of the public through the school website. Unless there are legislative or regulatory changes in the interim, this policy will be reviewed yearly.	

Scope of the Policy

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

The Education and Inspectors Act 2006 empowers Headteachers 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 online 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 regards to the searching for an end of electronic devices and the deletion of data.

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This policy should be read alongside the Academy's Child Protection and Safeguarding Policy and Keeping Children Safe in Education 2026. All staff, including staff who do not work directly with children, are required to read Part One of KCSIE in full and understand their safeguarding responsibilities.

Roles and Responsibilities

Governors - The Pupil and Staff Welfare Committee

The Pupil and Staff Welfare Committee (PSWC) are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness. This will be carried out by the PSWC receiving regular information about online safety incidents and monitoring reports. The PSWC will:

- regularly monitor online safety incident logs
- regularly monitor filtering/change control logs

Principal and Senior Leaders

The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead (DSL).

The Principal and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

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

The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

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

Online Safety Lead

The Online Safety Lead (Clemency Price) will

- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority where appropriate
- liaise with school technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meet regularly with the Deputy Designated Safeguarding Leads to discuss current issues, review incident logs and filtering/change control logs
- attend relevant meetings

Network/Technical Staff

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority and Academy safety policy and guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks, internet, digital technologies, and emails are regularly monitored in order that any misuse or attempted misuse can be reported to the Principal/ Senior Leaders for investigation, action and sanction
- that monitoring software/systems are implemented and updated as appropriate.

The Academy recognises the importance of maintaining effective filtering and monitoring systems in line with Department for Education Filtering and Monitoring Standards. Filtering and monitoring systems are regularly reviewed by safeguarding and technical staff to ensure they remain effective, proportionate and responsive to emerging safeguarding risks. Concerns identified through monitoring processes are escalated appropriately and may inform safeguarding intervention, staff training, curriculum development and wider pastoral support.

An effectiveness review of filtering and monitoring will be undertaken at least annually by the senior leader responsible for filtering and monitoring, with support from the DSL and IT/technical staff. The review will include checks across all internet-connected devices and relevant locations, including pupil-accessible devices and, where applicable, personally owned devices connecting to Academy systems. A written record of the review, findings and actions will be maintained and reported through safeguarding/governance arrangements.

Teaching and Support Staff

Teachers and support staff are responsible for ensuring that:

- they have up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood, and accept the staff Acceptable Use Policy (AUP), to help remind staff of the AUP. The Academy has set up a pop up to appear on screen every term on all school computers. Once staff have read and accepted this, they will confirm by selecting the **Accept** button. If they choose **Decline**, they will be denied access to the network and will be automatically logged out of the computer
- they report any suspected misuse or problem to the Senior Leader responsible for online safety for investigation, action, and sanction
- all digital communications with pupils, parents/carers should be professional and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety, and Acceptable Use policies
- pupils have a good understanding of research skills, upholding copyright regulations and the need to avoid plagiarism
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices
- 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.

Designated Safeguarding Lead (DSL)

Our school DSL is Lorna McCurdy, Assistant Vice Principal - Pastoral. The DSL training includes online safety issues and awareness of the potential for serious child protection and/or safeguarding issues to arise from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate online contact with adults, strangers, and people they may know
- potential or actual incidents of grooming
- online or cyberbullying

Pupils

All pupils are responsible for ensuring that:

- are responsible for using the school digital technology systems in accordance with the Acceptable Use Agreement
- they have read, understood, and accept the Acceptable Use Policy (AUP), to help remind them of the AUP. The Academy has set up a pop up to appear on screen every term on all computers. Once a user has read and accepted this, they will confirm by selecting the **Accept** button. If they choose **Decline**, they will be denied access to the network and will be automatically logged out of the computer
- they have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- they 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 and use of images and on online or cyberbullying

- they understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Academy's online safety policy covers their actions out of school, if related to their membership of the Academy.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet, digital and mobile devices in an appropriate way. The Academy will work with families to help them understand these issues through parents' evenings, newsletters, letters, website, social media, and information about local, national and global online safety campaigns/relevant updates.

Parents/carers will be encouraged to support the school in promoting good online safety practices, and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the school (where this is allowed).
-

Pupils will be educated regarding the safe, responsible and ethical use of artificial intelligence (AI) and generative technologies. This includes developing an understanding of the risks associated with:

- AI-generated content
- Misinformation, deepfakes
- Plagiarism
- Privacy concerns
- Inappropriate use of AI platforms.

Pupils will be supported to critically evaluate online information and understand that AI tools must not replace independent thinking, learning or safe online behaviours.

Generative AI

- pupil use of generative AI must comply with age restrictions of the particular product;
- pupil-facing AI tools must be appropriately safeguarded;
- staff should use only Academy-approved AI tools where appropriate;
- safeguarding, privacy/data-protection and intellectual-property risks must be considered before introducing AI tools;
- AI tools accessible to pupils must be considered within filtering and monitoring arrangements;
- staff and pupils should understand the risks of AI-generated misinformation, manipulation, deepfakes and harmful or sexualised imagery;
- AI-generated or digitally altered sexual imagery involving children is treated as a safeguarding matter.

Online Safety Risk Assessment and Monitoring

The Academy recognises that online risks evolve rapidly and therefore maintains a separate Online Safety Risk Assessment and Action Plan which is reviewed termly by safeguarding and the IT, Data and Systems manager.

The risk assessment identifies:

- emerging online safeguarding risks
- filtering and monitoring effectiveness
- contextual safeguarding concerns
- risks linked to vulnerable learners
- AI-generated/deepfake imagery/chatbot/relationship-simulation risks
- AI-enabled manipulation/ effectiveness of filtering/monitoring of AI tools
- emerging online platforms/features
- trends identified through CPOMS and behaviour systems
- areas requiring further action or staff training

The DSL, Online Safety Lead and IT, Data and Systems manager meet regularly to review:

- filtering and monitoring reports
- attempted breaches or bypasses
- safeguarding incidents
- online safety trends
- emerging risks linked to technology and social media
- generative AI and AI-enabled features embedded in other platforms.

The following questions are considered as part of this review:

- Which AI tools can pupils access?
- Are they age-appropriate?
- Are they filtered/monitored?
- Can pupils access them through personal devices?
- Are safety controls still effective when using an Academy account?
- Are harmful prompts/searches generating alerts?
- Is the DSL receiving relevant safeguarding alerts?
- Have DPIAs been completed where appropriate?

Outcomes from monitoring activities are reported to senior leaders and governors as part of safeguarding oversight arrangements.

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 and digital literacy, is therefore an essential part of the Academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum, and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities.

The 4 Cs of Online Safety

The Academy recognises that online safety risks can be considered through four broad categories: Content, Contact, Conduct and Commerce. These categories will be used to support the planning of online safety education, safeguarding responses and the Academy's assessment of emerging online risks.

- **Content** – pupils may be exposed to harmful, inappropriate or illegal material, including pornography, violent or extremist content, misinformation and disinformation, and harmful or inappropriate content generated or manipulated using artificial intelligence (AI).
- **Contact** – pupils may experience harmful or inappropriate contact with other people online, including strangers, adults, peers or others seeking to manipulate, groom, exploit or otherwise cause harm.
- **Conduct** – pupils may experience or participate in harmful online behaviour, including bullying, harassment, coercive or controlling behaviour, sharing of images without consent, the creation or sharing of nudes or semi-nudes, and AI-generated or digitally altered images.
- **Commerce** – pupils may be exposed to financial or commercial risks online, including scams, fraud, inappropriate advertising, in-app purchases, gambling-related content and other forms of financial exploitation.

Online safety education will address these areas in an age-appropriate and developmentally appropriate way. Pupils will be taught how to recognise risks, make informed and responsible choices, protect themselves and others, and know how and where to seek help when they encounter harmful online content or behaviour.

Our online safety curriculum will be provided in the following ways:

- a planned online safety curriculum should be provided as part of Computing, iMedia and Computer Science; INSIGHT and mentor time activities and should be regularly revisited
- key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities
- pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- pupils should be taught to acknowledge the source of information used and to respect copyright regulations when using material accessed on the internet
- 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 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
- in lessons where internet use is pre-planned, it is best practice that 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.
- where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education - Parents/Carers

Many parents and carers have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children, including the monitoring and/or regulation of the children's online behaviours. Parents/carers 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, website and other Academy communication media
- Parents/carers consultation evenings
- High profile events/campaigns e.g., Safer Internet Day
- Reference to the relevant websites and publications such as (list is not exhaustive):
    - SWGfL - www.swgfl.org.uk
    - Safer Internet - www.saferinternet.org.uk/
    - Childnet - http://www.childnet.com/parents-and-carers
    - NSPCC – https://www.nspcc.org.uk/keeping-children-safe/online-safety/
    - CEOP - https://www.ceop.police.uk/Safety-Centre/private-sector/

Education & Training – Staff

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

- All new staff should receive online safety training as part of the induction programme, to ensure that they fully understand the Academy's Online Safety Policy and Acceptable Use Agreement
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL, Local Authority and other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be presented to staff in meetings, professional development and training sessions
- The Online Safety Lead will provide advice, guidance and training to individuals as required.

Technical-Infrastructure/Equipment, Filtering and Monitoring

The Academy 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:

- IT and technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems, and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Academy technical systems, the network, and devices
- All users will be provided with a username and secure password by the Network Manager who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password
- The administrator passwords for the Academy systems used by the Network Manager must also be available to the Principal or another nominated senior leader and kept in a secure place
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and those regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored
- Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- The Academy has provided enhanced user-level filtering
- Technical staff regularly monitor and record the activity of users on the school network, and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place for users to report any potential or actual technical incident or security breach to the relevant person
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the network and data. These are tested regularly. The infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff/pupils) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the
- internet or taken off the school site unless safely encrypted or otherwise secured.

Cyber security is considered a safeguarding matter because cyber incidents, data breaches or disruption to digital services may directly affect the safety and welfare of pupils and staff.

Mobile Devices

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.
All users should understand that the primary purpose of using mobile/personal devices in a school context is educational. This policy is consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

Mobile Phone Policy

All mobile phones brought into the Academy are done so at the pupil's own risk. All mobile phones must be locked in a pouch before the pupil enters the school building.

The aims of the mobile phone policy are:

1) To be compliant with DfE statutory guidance introduced in June 2026 that all schools should be mobile phone-free environments by default.
2) To ensure pupils do not to have access to mobile phones throughout the school day, including lessons, time between lessons, breaktimes and lunchtime.
3) To ensure that all classrooms are learning spaces, that avoids distractions from mobile phones

Mobile phones can be used in the following areas only:

1. Sixth Form Study Areas (for Sixth Formers only)

Consequences for pupils not following the above policy:

- If a pupil's phone is found in their possession not in a pouch the following consequence will apply: -3 behaviour points, 90 minute SLT detention and phone confiscation until 3:30pm on the day of confiscation.
- If a pupil is seen using their phone in school the following consequence will apply: -3 points, Isolation sanction for the rest of the day and phone confiscation until 3:30pm on the day of confiscation.
- If a pupil refuses to hand over their phone for confiscation the following consequence will apply: parents contacted to attend the Academy and remove the phone. If this is unsuccessful the pupil will be suspended from the Academy.

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. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about
potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school 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 to ensure 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 without prior consent being obtained.

Communication

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

The Academy recognises that online safeguarding risks continue to evolve and may present through social media platforms, gaming, messaging applications and other emerging technologies. Current contextual safeguarding concerns include:

- Bullying
- Misogyny
- Harmful influencer content
- Coercive or controlling behaviours

- Sextortion
- Exploitation
- Radicalisation
- Exposure to harmful sexualised content
- The making or sharing of nudes or semi-nudes

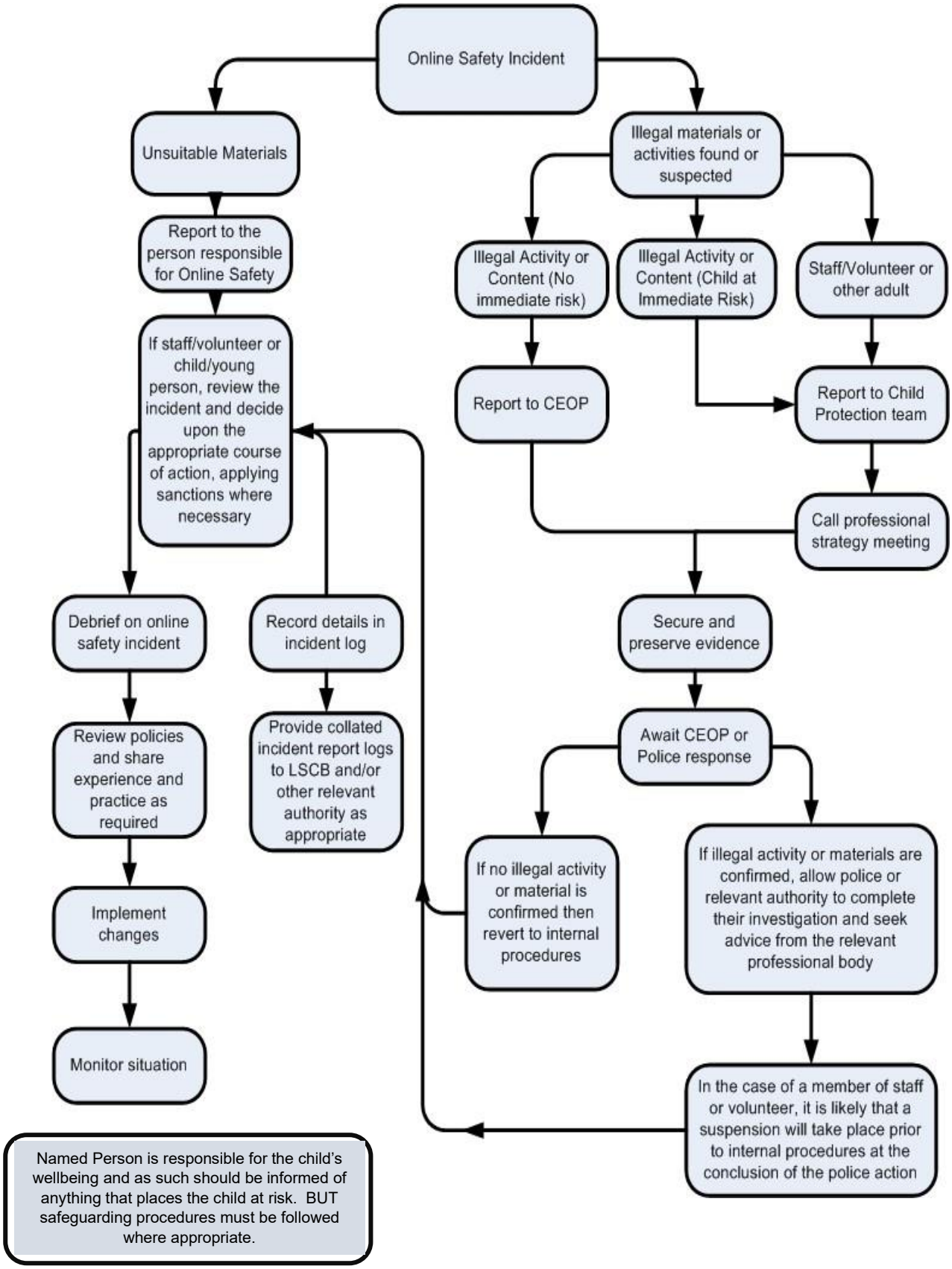
The making or sharing of nudes or semi-nudes includes the following:

- Photographs
- digitally altered images
- AI-generated images
- deepfakes
- images created without the child having originally taken a photograph

Staff receive regular safeguarding updates to ensure that emerging online risks are identified, understood and responded to appropriately.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child sexual abuse material (CSAM) or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse- see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

    1. Internal response or discipline procedures
    2. Involvement by Local Authority or national/local organisation (as relevant).
    3. Police involvement

- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

    1. incidents of 'grooming' behaviour
    2. the sending of obscene materials to a child
    3. adult material which potentially breaches the Obscene Publications Act
    4. criminally racist material
    5. promotion of terrorism or extremism
    6. other criminal conduct, activity, or materials
    7. offences under the Computer Misuse Act (see User Actions chart above)

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Pupil Acceptable Use Policy Agreement

The use of ICT has an enormous impact on the academic progress that pupils make and will certainly feature strongly when our pupils leave us and enter higher education or take up employment. Within the Academy we will use a wide range of software including subject specific software. There has also been increasing need to use other technologies such as online audio and video recordings within lessons due to provisions made available to pupils as a result of the Covid-19 pandemic.

Whilst the internet is a fantastic resource it is essential that pupils learn to use it appropriately. In order to keep pupils safe, we actively monitor the use of ICT continuously and will prevent access to those sites we deem unsuitable (for example sites that are pornographic, racist or violent). Pupils will be given an individual username and password to access their own work area which they **must not share** with others.

Shown below is the Academy's 'Acceptable Use Policy' which sets out what is expected from pupils using ICT equipment. **They will only be able to continue to access the network if they agree to follow these rules**. Please take time to read through this with your son / daughter and ensure that they understand it before completing and returning it to your child's Mentor.

The Academy have high expectations about being **respectful towards** staff and pupils. It is **not acceptable** to send memes/ similar images of staff or pupils within the Academy. These images may cause offence and /or upset. Sending such images will **not** be tolerated.

Rules for the Responsible Use of ICT equipment

The Academy allows access to ICT equipment, Google Classroom, Microsoft Teams and the Internet (including on my own device) to help and assist with our learning.

These rules will keep everyone safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret and secure;
- I will not access other people's files;
- I will only use the computers for Academy work and for homework;
- I will not bring in CD's, memory sticks or other computer media from outside school unless I have been given permission from my teacher;
- I will only e-mail or message people I know, or that my teacher has approved;
- The messages I send will be polite and responsible;
- I will not send any threatening messages that could be considered as cyberbullying;
- I will not create / send or share memes or images of staff or students;
- I will not publicly give out my home address or telephone number, or arrange to meet someone I do not know.
- I will not record (video or audio) anyone using equipment without their consent;
- I will report any unpleasant material or messages sent to me to my teacher / mentor;
- I understand that the Academy's policy for behaviour still applies to learning both in the classroom and on Google Classroom / Microsoft Teams;
- I understand my report would be confidential and would help protect other pupils and myself;
- I understand that the Academy will monitor the files in my user area and the Internet sites I visit;
- I understand any files stored on my user area will be removed without consent if found to be inappropriate / against the Acceptable Use Policy;
- I understand that failure to comply with the Acceptable Use Policy will result in a temporary or permanent ban to access of the Academy's ICT services.

Staff Acceptable Use Policy Agreement

(Note: this policy applies to all staff, volunteers, community users and governors)

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school's systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff 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 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 Haberdashers' Abraham Darby 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, Teams etc.) out of school, and to the transfer of staff and pupil/pupil personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use.
- 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 use strong passwords (at least eight characters long and containing special symbols) and will change my passwords on a regular basis.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the ICT Support team.
- I will ensure that I do not leave any device unlocked while unattended.
- All portable devices I use to access school systems will be password/passcode protected.
- Computer workstations will be positioned so that they are not visible to casual observers.

I will be professional in my communications and actions when using the school's ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Haberdashers' Abraham Darby:

- If I use my 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. All mobile devices will be password/passcode protected.
- 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 understand that data in the appropriate place is backed up and secure. Data stored elsewhere might not be backed up.
- 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in the school's policies.
- I will only transport, hold, disclose, or share personal information about myself or others, as outlined in the School's Data Protection Policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil / 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 suspected data breach to the school's Data Protection Coordinator.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened to the schools ICT Support team.

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 Haberdashers' Abraham Darby:

- 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.

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.

Links with other Academy Policies

This policy links to the following policies and procedures:

- Behaviour Policy (including Anti-Bullying Policy)
- Data Protection Policy
- Safeguarding Policy
- Staff code of conduct
- Acceptable Use Policy