HILTON
SPENCER ACADEMY

Peacroft Lane, Hilton, Derby, DE65 5GH
01283 732 334
info@hiltonspencer.com
hiltonspencer.com
@hiltonprimary

Online Safety Policy

Online Safety Lead: Gary Staddon

Designated Safeguarding Lead: Tricia Edwards

Designated Deputy Safeguarding Leads: Shelley White, Claire Wright, Gary Staddon, Katie Brown

Computing Lead: Rebecca Brooks-Sutton

Network Manager: Lorraine Kaylor

Policy Reviewed and Updated – October 2021

Next Review – October 2022

About this policy

Policy Aims

The online safety policy has been developed within The Spencer Academies Trust, based on a template provided by Education People, and with reference to local authority advice and Safeguarding Children Partnership procedures. It takes into account DfE statutory guidance documents 'Keeping Children Safe in Education' , Early Years and Foundation Stage and 'Working Together to Safeguard Children.'

The purpose of the online safety policy is to:

- Safeguard and protect all members of the school community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

At Hilton Spencer Academy we recognise that the issues and risks associated with online safety can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

The online safety policy has been drafted to address each of these areas of risk.

Policy Scope

- Hilton Spencer Academy recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- We understand that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Hilton Spencer Academy believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Code of conduct/staff behaviour policy
- Behaviour policy
- Safeguarding and Child Protection policy
- IT data protection, security and acceptable use policies

Peacroft Lane, Hilton, Derby, DE65 5GH
01283 732 334
info@hiltonspencer.com
hiltonspencer.com
@hiltonprimary

Roles and Responsibilities

The Designated Safeguarding Lead (DSL), Tricia Edwards, has lead responsibility for ensuring online safety, working with DSL deputies and members of the leadership team in school.

Hilton Spencer Academy recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to executive leaders within The Spencer Academies Trust
- Review and update online safety policies on a regular basis (at least annually) with stakeholder input.

All staff will:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

The Trust's appointed IT contractors/trained IT technicians in school will:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and Engagement

Education and engagement with learners

Hilton Spencer Academy will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and e-security programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use (SMART) posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Using support, such as external visitors and membership of 'National Online Safety', where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Learners

Hilton Spencer Academy recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Hilton Spencer Academy will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum, Hilton Spencer Academy will seek input from specialist staff as appropriate, including the SENCO, or Special Needs Coordinator.

Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

Hilton Spencer Academy recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that parents and carers read online safety information as part of the school community.
- Encourage parents and carers to read our acceptable use policies and discuss the implications with their children.

Reducing Online Risks

Hilton Spencer Academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at pace.

We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom Use

Hilton Spencer Academy uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, web cams and video cameras

All devices owned by the school or Trust will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

Members of staff will evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. IT technical staff will support evaluation and the training and processes necessary to ensure that learning resources are appropriate for use.

Hilton Spencer Academy will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage

Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Key Stage 1 and 2

Learners will use age-appropriate search engines and online tools.

Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

Managing Internet Access

We will maintain a record of users who are granted access to our devices and systems.

All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

We will carry our regular audits and audit activity to help identify pupils trying to access inappropriate content to establish any vulnerabilities and offer advice, support and react accordingly.

Filtering

We use *Smooth Wall* which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature

The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

We work with our appointed external IT contractors and IT technicians in school to ensure that our filtering policy is continually reviewed.

If learners discover unsuitable sites, they will be required to:

- Turn off the screen and report the concern immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or CEOP.

Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

Monitoring will be carried out using the *Smoothwall* Internet Filtering system.

A log file request will then be need to be sent to the IT provider who will then provide this information.

If a concern is identified via monitoring approaches we will:

- DSL or deputy will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Full information can be found via the data protection pages and policies which can be found at www.satrust.com

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network.
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all but the youngest users and children with SEND.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

Use of staff email/class dojo

Members of staff are encouraged to have an appropriate work life balance when responding to email or messages via class dojo, especially if communication is taking place between staff, learners and parents.

Members of staff will refer to and adhere to the acceptable use policy and other relevant policies.

Learners will use provided individual dojo accounts for educational purposes. Learners will sign an acceptable use policy and will receive education regarding safe and appropriate etiquette before access is permitted.

Whole-class or group dojo messages may be used for communication outside of the setting.

Educational use of videoconferencing

Hilton Spencer Academy recognise that videoconferencing and use of webcams presents potential IT security and data protection risk, whilst entailing a wide range of learning benefits.

- All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
- Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.
- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering any videoconference call or message
- Videoconferencing will be supervised appropriately, according to the learner's age and ability
- Unique log on and password details for school videoconferencing services will only be issued to members of staff where this is found to be appropriate following risk assessment, and should be kept securely, to prevent unauthorised access
- Any use of videoconferencing as a meeting tool with an individual child will be assured by the presence of a parent/carer. Not less than two members of staff should be present.

Recorded videocall content

When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given, and any recorded material stored securely only until such time as the legal basis for retaining recordings is no longer in place.

If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

Management of Learning Platforms

Hilton Spencer Academy uses class dojo as its official learning platform.

Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.

Only current members of staff, learners and parents will have access to the LP. An exception may be made for children registered to join the school and taking part in transition programmes, in which case access will be granted for this purpose.

When staff and learners leave the setting, their account will be disabled or transferred to their new establishment.

Learners and staff will be advised about acceptable conduct and use when using the LP.

All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- A learner's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

Management of Applications (apps) used to record pupil progress

We use *Google Drive* as a tool to monitor learner progress. Under Trust processes, all information which may be accessed from outside the school or transferred between sites must be anonymised.

It is the responsibility of the Trust Data Director to ensure that the appropriate safeguards and processes are in place to ensure data security for learner progression.

The Principal holds ultimate responsibility for the security of any data or images held of pupils as part of their education. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data:

- Only school issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Social Media

Expectations

The expectations' regarding safe and responsible use of social media applies to all members of Hilton Spencer Academy community.

Members of staff will refer to and adhere to the school social media policy and any other policy where the staff use of social media is referred to.

We will control learner and staff access to social media whilst using setting provided devices and systems on site.

Concerns regarding the online conduct of any member of Hilton Spencer Academy community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.

Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour policies.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Learners will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

School Use of Social Media

School and staff-sanctioned use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

Staff will use Trust-provided email addresses to register for and manage any official social media channels only.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Any official social media activity involving learners will be moderated to ensure use contingent with images, data protection and other IT security policies.

We will ensure that use of social media for communications does not exclude members of the community who are unable or unwilling to use social media channels.

Learners Use of Personal Devices and Mobile Phones

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

At Hilton Spencer Academy use of learners' personal devices and mobile phones is not allowed in school.

If a learner needs to contact his/her parents or carers they will be allowed to use the office phone.

Parents are advised to contact their child via the school office.

Mobile phones or personal devices will not be used by learners during lessons or formal educational time.

If a pupil breaches the policy, the phone or device will be confiscated and will be held in a secure place.

Searches of mobile phone or personal devices will only be carried out in accordance with Dfe guidance and our policy. *See* www.gov.uk/government/publications/searching-screening-and-confiscation)

Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. *See* www.gov.uk/government/publications/searching-screening-and-confiscation)

Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.

If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) of any breaches our policy.

Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.

Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers and learners to work in partnership to resolve online safety issues.

After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

We will refer to the flow chart on responding to incidents of misuse, made available in the Online Safety File on the Staff Shared Drive (Hilton Spencer Academy's Network) and in Appendix A of this policy.

Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Principal will liase with police to ensure that potential investigations are not compromised.

Concerns about Pupil Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with local Safeguarding Children Board thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

Hilton Spencer Academy has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.

Hilton Spencer Academy recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

Hilton Spencer Academy recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

Hilton Spencer Academy also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

Hilton Spencer Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.

If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.

Implement appropriate sanctions in accordance with our behaviour policy.

Inform parents and carers, if appropriate, about the incident and how it is being managed.

If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.

If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

If a criminal offence has been committed, the DSL (or deputy) will discuss this with Police first to ensure that investigations are not compromised.

Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

Hilton Spencer Academy recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".

Hilton Spencer Academy will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.

If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.

Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

Act in accordance with our child protection policies and the relevant local authority Safeguarding Child Board's procedures.

Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Store the device securely.

If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.

Inform parents and carers, if appropriate, about the incident and how it is being managed.

Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

Hilton Spencer Academy ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

Hilton Spencer Academy Hilton Spencer Academy Hilton Spencer Academy recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

Act in accordance with our child protection policies and the relevant local authority Safeguarding Child Board's procedures.

If appropriate, store any devices involved securely.

Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform police via 101, or 999 if a child is at immediate risk.

Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).

Inform parents/carers about the incident and how it is being managed.

Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police by using 101.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).

If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from police first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

Hilton Spencer Academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police using 101.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant local authority Safeguarding Children Partnership Safeguarding procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), police or the LADO.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the Police via 101 (999 if there is an immediate risk of harm) and Children's Services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the principal is informed in line with our managing allegations against staff policy immediately and without any delay.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

Online and cyber-bullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Hilton Spencer Academy. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

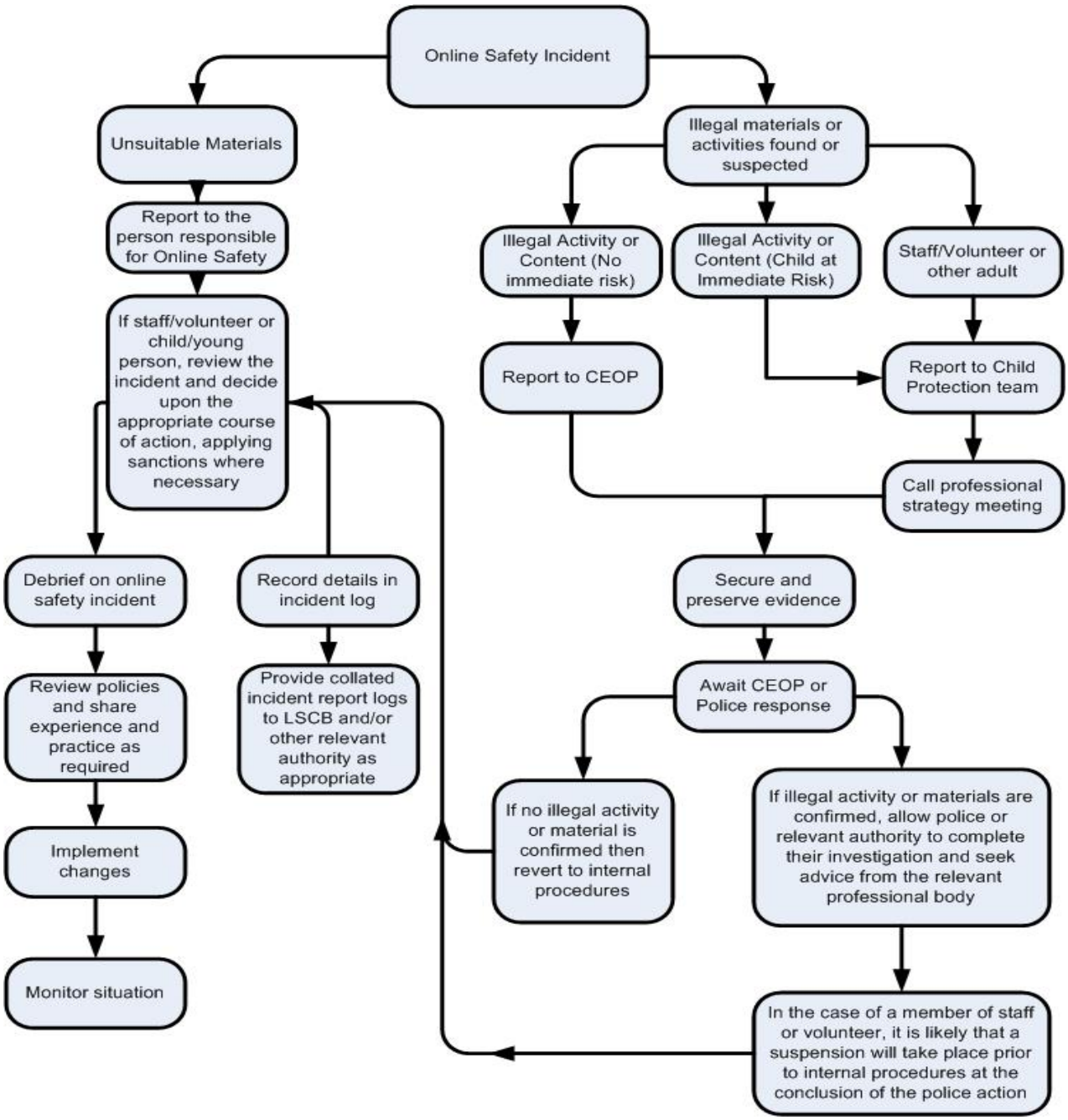
Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and prevent pathway which may include a referral into Channel.

If we are concerned that member of staff may be at risk of radicalisation online, the principal be informed immediately, and action will be taken in line with the child protection and allegations policies.

Appendix A: Responding to incidents of misuse – flow chart



Appendix B: Resources

Derby City & Derbyshire Safeguarding Children Partnership on line procedures DDCSP:

http://derbyshirescbs.proceduresonline.com/

Police:

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Police via 101

LADO

By referral into Professional.Allegations@derbyshire.gov.uk

Form found here http://derbyshirescbs.proceduresonline.com/docs_library.html

Call Derbyshire (Starting Point)

Immediate risk of harm phone 01629 533190

For all other referrals complete an online form https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx

For professional advice phone 01629 535353

National Links and Resources for Educational Settings

CEOP:

www.thinkuknow.co.uk

www.ceop.police.uk

Childnet: www.childnet.com

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

360 Safe Self-Review tool for schools: www.360safe.org.uk

Peacroft Lane, Hilton, Derby, DE65 5GH
01283 732 334
info@hiltonspencer.com
hiltonspencer.com
@hiltonprimary

National Links and Resources for Parents/Carers

Action Fraud: www.actionfraud.police.uk

CEOP:

www.thinkuknow.co.uk

www.ceop.police.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

UK Safer Internet Centre: www.saferinternet.org.uk