Abingdon Primary School Digital Resilience Policy Date: 2020

Date of policy: June 2020

Date of next review: September 2021

Member of staff responsible for overseeing that this policy is implemented and regularly reviewed: Ruth Hill/Raj Kaur

This policy sets out the ways in which the school will:

- Educate all members of the school community on their rights and responsibilities with the use of technology;
- Build both an infrastructure and culture of digital resilience;
- Work to empower the school community to use the Internet as an essential tool for lifelong learning.

The term Digital Resilience is used throughout this document in replacement of the outdated and overused term of 'E-Safety'

'Digital Safeguarding and Resilience' is a whole-school issue and responsibility. There is a 'duty of care' for any persons working with children or members of the school community to educate on these risks and responsibilities. 'Digital safeguarding' falls under this duty and this strategy aims to highlight this duty.

This policy purposely links closely to the school's policies on safeguarding and child protection, preventing radicalisation and bullying and behaviour.

This policy will be reviewed annually and will be under continuous revision in response to significant new developments in the use of technologies, new threats to digital safeguarding or incidents that have taken place.

Next review date is: September 2021

Contents

Cyberbullying

1.31 Strategy to deal with cyberbullying

1.32 How will we teach children about cyberbullying?

1.33 Resources to deal with cyberbullying

Online Gaming

1.34 Tips for parents regards online gaming

Youth Produced Sexual Imagery

1.35 Steps to take when dealing with an incident of youth produced sexual imagery

Reporting and Response to incidents

1.36 Handling complaints

1.37 Sanctions and Disciplinary proceedings

1.38 Useful sites

1.1 Use of policy

This policy applies to all members of the school community, including staff, pupils, volunteers, parents/carers, visitors and community users.

The school will manage digital resilience as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate online behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review

The Implementation of the digital resilience policy will be monitored by the digital safeguarding working group, meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by the digital safeguarding working group by looking at:

- The log of reported incidents
- The Internet monitoring log
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

1.2 Communicating school's strategy

This strategy will be available from the school's website for parents, staff, and pupils to access as and when they wish. Rules relating to the school's expectations of conduct for both staff and students are displayed around the school.

1.3 Digital Resilience

Digital Resilience is a term given to "the social and emotional literacy and digital competency to positively respond to and deal with any risks that pupils might be exposed to when they are using social media or going online"

Being digitally resilient is about being able to deal with any incidents that go awry online especially on social media, we aim to equip our pupils with the emotional resources needed to:

- Understand when they are at risk online
- Know What to do and where to go to seek help
- Learn from past experience and actions of both themselves and others
- Recover when things do go wrong

Digital safeguarding is integrated into the curriculum where the internet or technology are being used. Particularly during PSHE lessons and assemblies where personal safety, responsibility, and/or development are being discussed.

1.4 Responsibility & Accountability

Head Teacher & Senior leadership team will:

- Ensure that all existing and new staff are familiar with the schools digital safeguarding strategy and its guidance and code of conduct when using social networking and ICT.
- The Computing Coordinator will:
- Devise, update and monitor the school's use of the ICT skills progression.
- Explore innovative ways to use computers to teach creatively, communicate with all stakeholders and enrich learning.
- Support teachers with planning and use of resources.
- Undertake appropriate professional development to ensure an up to date knowledge and report to staff.
- Keep informed and responsive to technological developments and advancements
- Lead staff professional development in staff.
- Manage the computing resources in the school.
- Monitor teaching, learning and standards in Computing.
- Produce an action plan for Computing, setting out the priorities which will be incorporated in any school improvement plan.
- Carry out any risk assessments and follow this strategy.

Staff will:

- Should ensure that they are familiar with the contents of the Digital Safeguarding Strategy and the schools expected standards and guidance on the use of ICT.
- Follow health and safety guidelines and this strategy.
- Plan opportunities for the relevant and creative use of ICT across the curriculum on an ongoing basis.
- The Head teacher is responsible for ensuring the safety of all members of the school community.

The Computing coordinator will work with the Head teacher and the Designated Safeguarding Lead, to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying.

A digital safeguarding working group will work with the Digital Safeguarding Leader to implement and monitor the digital resilience policy and AUPs (Acceptable User Policies and Children User agreement policies).

Position	Key roles/responsibilities
Head Teacher and governors	Ensure that the Digital Safeguarding Strategy is implemented and compliance monitored. Ensure that the appropriate roles and responsibilities of the school digital safeguarding structure are in place. Ensure regular reports of the monitoring outcomes on digital safeguarding are reported on the CPOMS system and to the Governing Body.
Designated Safeguarding Lead Adam Cooper	The DSL (Adam Cooper) takes lead responsibility for child protection and wider safeguarding. The DSL will be available during school hours for staff to discuss any safeguarding concerns. The DSL can also be contacted out of school hours by mobile phone
Computing Lead Raj Kaur Digital Safeguarding working group Raj Kaur Danny Barstow (CEOP trained) Keith Smith Farida Bashir	Ensure up-to-date with latest developments and issues of concern, publicising these appropriately to staff, students and parents. Monthly meeting (same day and time where possible) for updates and actions to move forward. Be in receipt of all digital safeguarding concerns. Keep logs of any reported incidents on CPOMS and actions taken to resolve these.
• All staff	All staff will understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. All staff need to work to agreed guidelines and have a "front line" monitoring and reporting role for incidents. Understand that any concerns should be reported to the Safeguarding Leads for recording on CPOMS. • All staff will undertake annual 'digital safeguarding' training with local authority. Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the AUP and Digital Resilience Policy • • Report any suspected misuse or concerns to the Digital Safeguarding Leader and check this has been recorded

	• Provide appropriate Digital Resilience learning opportunities as part of a progressive Digital Resilience curriculum and respond • Model the safe use of technology • Monitor ICT activity in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	• Read, understand and sign the Pupil AUP and the agreed class Internet rules • Participate in Digital Resilience activities, follow the AUP and report concerns for themselves or others • Understand that the Digital Resilience Policy covers actions out of school that are related to their membership of the school
Parents and Carers	• Encourage (by signature) the Pupil AUP • Discuss Digital Resilience issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the Internet • Access the school website in accordance with the relevant school AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any Digital issues that relate to the school • Maintain responsible standards when using social media to discuss school issues
Technical support provider	• Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack

	• Ensure users may only access the school network through an enforced password protection policy • Keep up to date with digital technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the Digital Safeguarding Leader for investigation • Ensure monitoring systems are implemented and updated • Ensure the school's web filtering solution is compliant with the Government's Prevent Strategy (March 2015) • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities
Community users	• Sign and follow the Guest/Staff AUP before being provided with access to school systems

1.6 How will we teach about digital safeguarding ?

- Rules for using the internet will be discussed with all pupils at the start of each year either through circle time or taught via taught lessons.
- Pupils are informed that network and internet is monitored and inappropriate use is followed up
- Pupils receive digital safeguarding lessons through the computing curriculum, PSHE lessons, circle time and other curriculum areas and are constantly reminded of being safe online and being a good digital citizen. Within this:
- Key Digital Resilience messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all lessons
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the School's scheme of work
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material

- In lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in Internet searches

- Pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet

- Pupils will write and sign an AUP for their class [which might be agreed class rules] at the beginning of each school year, which will be shared with parents and carers

- Pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'.

1.7 How will we teach about Digital Safeguarding in SMSC and other curriculum areas?

There are explicit links and overlaps between teaching about Digital Safeguarding within computing curriculum and personal, social and health education, citizenship, other curriculum areas, assemblies and external visitors the school utilises a PSHE programme from Family Planning Association which teaches children, details of schools PSHE programme of study in relation to Digital Safeguarding.

At Abingdon we aim to ensure that our teaching of the computing curriculum and does not only concentrate things such as coding, algorithms and processes but also teaches the social elements of life online including how to critique content, recognise fake news, how to assess body image such as taking 'selfies' and how to control one's online activity and when this becomes problematic.

1.8 Education and information for parents and carers

Parents and carers will be informed about the ways the Internet and technology is used in school. They have a critical role to play in supporting their children with managing online risks at home, reinforcing key messages about Digital Resilience and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance which they are asked to sign with their children and regular newsletter and website updates;

- Raising awareness through activities planned by pupils;

- Inviting parents to attend activities such as e-safety week, e-safety assemblies, digital parent's meetings or other meetings as appropriate;

- Providing and maintaining links to up to date information on the school website

1.9 Training of Staff and Governors

Acceptable use

- All ICT use in school should follow these guidelines and staff will be expected to be diligent and use their professional judgment.
- All staff and pupils will be expected to sign up to their own individual Acceptable use agreement Concerns may be addressed to the subject leader or Head Teacher
- Pupil inappropriate internet or ICT system use will be dealt with in line with the schools Bullying and Behaviour Polices.
- Staff inappropriate internet or ICT use will be dealt with in lines with the school's local authorities disciplinary procedures.
- All staff will have access to this digital safeguarding strategy and reminded of its importance.
- Staff will be made aware that internet traffic is monitored.
- Discretion and professional conduct is essential
- Staff must always use a child friendly safe search engine when accessing the internet with pupils
- You Tube use within the school on all devices is set at restricted use, this helps screen out any potentially mature content

Management of School Information Technology System

1.10 Technical Infrastructure

The computer systems in Abingdon are managed by One IT Services and Solutions, who will provide IT support to Abingdon in respect of hardware, software, helpdesk, networks management, management information systems and web services, the core purpose of this service will be delivery of the school's ICT strategy by ensuring the development and delivery of quality ICT services. These services will include

- Broadband provision
- Website hosting
- Help and Support with Microsoft Office Systems
- Ensure security strategies be discussed with the school.
- Ensuring central backup solutions and disaster recovery plans
- Regularly reviewing the schools' networks to ensure that the system has the capacity to take increased traffic caused by Internet use.
- The security of the whole system will be reviewed with regard to threats to security from Internet access.

- **E-security ensuring all Abingdon pupil data is stored securely on the school's computer system.**
- **Management and support of the school's anti-virus protection, the schools uses antivirus**
- This software will be installed on all school's devices and updated automatically each time an update is released.
- Ensure the use of e-mail and attachments will be monitored closely.
- The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP.
- The School ICT systems are managed in ways that ensure that the school meets e safety technical requirements
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

- The downloading of executable files by users
- The extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
- The installing programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator
- The installation of up to date virus software

Access to the school network and Internet will be controlled with regard to:

- Users having clearly defined access rights to school ICT systems through group policies
- Users (apart from possibly Foundation Stage and Key Stage One pupils) being provided with a username and password
- Staff users being made aware that they are responsible for the security of their username and password; they must not allow other users to access the systems using their log on details
- The 'master/administrator' passwords are available to the Headteacher and kept in a safe place (school safe).
- Users must immediately report any suspicion or evidence that there has been a breach of security
- An agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this e-safety policy
- Key Stage 1 pupils' access will be supervised with access to specific and approved online materials
- Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities

The Internet feed will be controlled with regard to:

- The school maintaining a managed filtering service provided by an educational provider
- The school monitoring Internet use
- Requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team/ IT technician.
- Requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged
- Filtering issues being reported immediately

1.11 Data Protection

The school will:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices
- Ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- Any sensitive data sent by e-mail should be only sent to secure email address and/or password protected.

1.12 Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform (Class Dojo) and to provide information about the school on the website. The school will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites

- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images

- Make sure that images or videos that include pupils will be selected carefully with their knowledge

- Seek permission from parents or carers before images or videos of pupils are electronically published

- Encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission

- All parties must recognise that any published image could be reused and repurposed

- Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance

- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use

- Publish a policy regarding the use of photographic images of children which outlines policies and procedures including disposal and deletion.

1.13 The authorisation of Internet access

Abingdon Primary School grants internet access to all staff and all pupils. Parental permission will be required before children can access the Internet.

- Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based upon responsible use.
- At Key Stage 1, the majority of the access to the Internet will be by teacher or adult demonstration. However, there may be situations when children have supervised access to specific approved on-line materials.
- At Key Stage 2, Internet access will only be granted to a whole class as part of the scheme of work after suitable education in the responsible use of the Internet, this will be both in school and out of school for topics such as 'reading plus'.
- Parents will be informed that pupils will need to be provided with supervised Internet access.
- Parents will be asked to sign and return the acceptable use policy agreement as part of the pupil 'starter pack'.
- Pupils will have regular digital safeguarding lessons as part of their computing curriculum. They are taught how to keep themselves safe whilst online, what information must be kept private and what to do if they are worried about anything they see or hear online.
- Pupils are taught that the Internet can be used as a way to influence and persuade people. They learn that they need to be aware of the risk of online grooming and radicalisation and that organisations seek to radicalise young people through the use of social media and the internet.

- Pupils are taught how to build their digital resilience to sexual exploitation, radicalisation, youth produced sexual imagery and cyberbullying and who to report to if they are concerned by anything they have seen or heard on the internet.

1.14 The management of published content and the school's website

Our website creates an environment that develops great home and school links; it is viewed as a fantastic tool for communicating our school ethos to the wider community. It is also a valuable resource that inspires pupils to publish work to a high standard, for a very wide audience and allows staff, parents and pupils to keep up to date with school news. Our website can celebrate pupils' work, promote the school and publish resources for projects or homework.

Our website is in the public domain, and can be viewed by anybody online, ground rules are therefore important to ensure that content reflects the school's ethos and that information is accurate and well presented.

For security of staff and pupils the publishing of pupils' names beside photographs that identify individual pupils is viewed as inappropriate on school websites. While any risks might be small, the parents' perception of risk has been considered.

- The safeguarding lead will take overall editorial responsibility of the website and ensure that content is accurate and appropriate.

- We will ensure that content is accurate and quality of presentation is maintained.

- The point of contact on the web site should be the school address, email and telephone number. Personal information or individual e-mail identities will not be published.

- Photographs will be selected carefully should not identify individual pupils. Group activity shots will be used in preference to individual "passport" style images.

- Names of pupils will not be used anywhere on the Web site, particularly alongside photographs.

- Written permission and consent from parents will be sought before photographs of pupils are published on the school website.

1.15 Email code of conduct

Staff

- E-mail must only be used in school for educational purposes.
- Staff should only use official school email accounts to communicate with parents or external organisations.

- Emails sent from the school should be professionally and carefully written

- Ensure that the school uses a secure business email system for communication
- Ensure that personal information is not sent via unsecure email
- Ensure that governors use a secure email system
- Ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- Make users aware that email communications will be monitored by the school
- Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- Use email at KS1 through a group or class activity with an adult sending and opening emails
- Provide pupils at Key Stage 2 with a monitored individual educational school email address
- In line with the digital safeguarding strategy students should not reveal any personal information over email, or arrange to meet up with anyone they have met online
- Students will be taught to identify spam, phishing and viruses and that these can cause harm to the school's network as part of the computing curriculum.
- Only publish official staff email addresses where this is required

Mobile devices

1.16 With respect to mobile phones

- Inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils', unless they have the permission of the Headteacher
- Inform staff that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team
- Inform all that personal devices should be password protected
- Advise staff not to use their personal mobile phone to contact pupils, parents and carers. School should provide a mobile phone for contact when necessary.
- Inform visitors of the schools expectations regarding the use of mobile phones
- Maintain the right to collect and examine any phone that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection.

- Allow permission for mobile phones to brought to school if parent requests this but to be left at the office for the duration of the School day.

Pupils

- Pupils are not permitted under any circumstances allowed to bring mobile devices into the school, if a pupil is found with a device they can be legally confiscated by the Head Teacher under section 94 of the Education and Inspection Act 2006.

1.17 With respect to other personal devices

- The staff AUP will apply to staff using their own portable device for school purposes
- Enable and insist on the use of the school's Internet connection while on the school site
- Maintain the right to collect and examine any device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school Internet connection

Communication (including use of Social Media)

All staff to be made aware and have access to the Social Networking policy. With respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing.

1.18 Safeguarding pupils in the context of social media

While we understand that age limits usually apply on most social networking platforms, we recognise that some pupils may ignore these restrictions, frequently use and visit these online environments, sometimes even with full endorsement from parents. It is therefore highly important that we educate our pupils so that they can make their own informed decisions and take responsibility for their conduct online.

Abingdon School pupils are taught about these matters through the computing curriculum, personal, social and health education, citizenship, other curriculum areas, assemblies and external visitors the school, we aim to make digital citizenship the forth pillar of our children's education.

Our staff will be responsible for delivery of the Digital Safeguarding and Digital Resilience, parts of the computing curriculum will be CEOP - Think You Know trained and may use the Think You Know recommended resources as part of this education, among other recommended resources.

Our pupils will be taught about the overarching risks of visiting these environments, the dangers of uploading personal information and photographs to social networking environments, the type of contact this could expose them to and the difficulty on getting something taken down once it is in the public domain.

In addition, pupils will also be taught

- The dangers of using personal publishing and social networking applications such as blogs, wikis, social networking sites, bulletin boards, forums, video conferencing, chat rooms and instant messaging applications
- Contemporary advice on the dangers of using social networking applications
- If using social networking applications
- How terms and conditions work on downloading certain applications
- How to use social networking sites in safe and productive ways
- How to use the school's ICT responsibly
- How to be a good digital citizen
- How to be digitally resilient if something goes wrong and where to go and who to talk to if something or someone upsets them
- Not to publish hurtful, harmful or defamatory comments about others on social networking sites

1.19 Content of interactions

Staff must not make reference on social networking sites to the school, its staff, pupils or their families. If staff adhere to this recommendation then the personal content of an individual's social networking membership is unlikely to cause any concern for the school.
If employment of the school is referred to, then the information posted would need to comply with the conditions set out below.

Any references made to the school or its staff, pupils or their families should comply with the school's policies Equal opportunities, and bullying and harassment.

- Staff must not post information, comments or entries on social networking sites which could be deemed or indeed interpreted as confidential to the school, staff, pupils or their families which could be deemed or interpreted as derogatory, defamatory or discriminatory.

- Staff should not use the school logo on their own personal social networking accounts, and should not post any links to the school website nor post any photographic images that include pupils or members of staff.
- Staff must not download copyrighted of confidential information
- Staff must not express personal views which would be misinterpreted as those of the school.
- Staff must not commit the school to purchasing, acquiring goods or services without appropriate authorisation.
- When posting any information onto a social networking site, staff must not post any entry that puts their effectiveness to perform their normal duties at risk.

If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the school, which allow staff to raise and progress such matters. It is important to note that social networks are not the appropriate forum to raise such matters. Employees should discuss any concerns they have with the Head

Teacher or senior leadership team in the first instance. Guidance may also be available from human resources or trade unions.

1.20 Privacy and security

Staff are advised to check their security and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly.

In using social networking sites, staff are recommended to only post content that they would wish to be in the public domain, **even if the content is subsequently removed from a site it may remain available and accessible**. Staff should consider not only how content could reflect on them, but also on their professionalism and the reputation of the school as their employer. Even with privacy settings in place it is still possible that the personal details of staff may be accessed more broadly than the other networkers identified by them.

Any reference to such information by pupils and/or their families, which a staff member deems to be inappropriate or is concerned about, should be reported to the Head Teacher or senior leadership team in the first instance.

If a staff member becomes aware that that a pupil, o a group of pupils has made inappropriate, insulting, threatening or derogatory comments about them, or other staff on social networking application or site; they must report to the Headteacher or a senior member of staff so that the appropriate processes can be implemented.

1.21 Breaches

Staff found to be in breach of this strategy may be subject to disciplinary action, in accordance with the schools Staff discipline conduct and grievance procedures with potential sanctions up to and including dismissal.

Information shared through social networking sites, even on private spaces, is subjected to copyright, data protection, freedom of information, equality, safeguarding and other legislation. Where staff work in roles that are governed by professional bodies/professional codes of conduct; the professional rules relating to social networking applied to them may be more stringent than those within this strategy.

1.22 Parents, social networking and allegations against staff:

The Education Act 2011, Section 13, states that

- If an allegation has been made against a person who is employed or engaged as a teacher, it is a criminal offence to publish any information which may lead to the identity of the teacher who is subjected to the offence
- Publication includes any speech, writing, relevant programme or other communication method is addressed to the public at large. This would also include any social networking site.
- It is an offence to not only name the alleged offender (teacher) but also publish any information that could lead to the public at large identifying the teacher.

A wide range of communications technologies have the potential to enhance learning.

Specific safeguarding issues

1.23 Social Networking and Preventing Radicalisation

(Also refer to the Safeguarding and child protection policy)

The amount of terrorist and extremist content online is a growing concern, with the increasing threat of children and young people being radicalised. As a school we have an extremely important role to play in protecting our pupils whilst they are online. Under section 29 of the Counter-Terrorism and Security Act 2015, we are expected to demonstrate those under our care are being prevented from 'being drawn into terrorism" and "non-violent extremism"

1.24 How could our pupils become radicalised?

Young people may be vulnerable to a range of risks as they pass through childhood. They may be exposed to new influences and potentially risky behaviours, influence from peers, influence from older people and especially the internet as they may begin to explore ideas and issues around their identity, this usually occurs in adolescent years, but special attention should also be paid to early key stage years on educating about these issues.

There is no single driver of radicalisation, nor is there a single journey to becoming radicalised. The internet creates more opportunities to become radicalised to both left and right wing ideologies, since it's a worldwide 24/7 medium that allows you to find and meet people who share and will reinforce a child's opinions.

Single agenda political and extreme religious groups can provide a sense of family or support that children may feel is lacking in their lives. This desire for security could also be due to poverty, unemployment, social isolation or feelings of rejection by their own faith, family or social circle.

In some cases the trigger may be an event, either global or personal, such as being a victim or witness to a race or religious hate crime. Young people may also join these groups as a result of peer pressure and the desire to 'fit in' with their social circle.

However, it should also be remembered that not all young people that experience these factors adopt radical views.

1.25 Level of extremist content online

There is a wealth of Far-Right, Far-left and Islamic extremist material available online including; magazines, articles, blogs, images, videos encouraging hate or violence, posts on social media and, websites created or hosted by terrorist organisations.

There are also terrorist training materials and videos glorifying war and violence that play on the theme of popular video games such as 'Call of Duty: Black Ops'. These use highly emotive language and images created to play on the issues young people are struggling with such as identity, faith and belonging.

Voice-Over IP and access to devices such as headsets on gaming systems may also be used in the radicalisation process, with young people being encouraged to pursue violence in the real world from material they are viewing within a violent war game.

1.26 Why could social networking be a concern?

Our children may actively search, come across by accident or be persuaded by others to look for content that is considered radical. Social media sites, like Facebook, Ask FM and Twitter, can be used by extremists looking to identify, target and contact young people. It's easy to pretend to be someone else on the internet, so children can sometimes end up having conversations with people whose real identities they may not know, and who may encourage them to embrace extreme views and beliefs.

Often children will be asked to continue discussions, not via the mainstream social media, but via platforms, such as Whatsapp, Kik Messenger and Whisper. Moving the conversation to less mainstream platforms can give users a greater degree of anonymity and can be less easy to monitor.

People who encourage young people to do this are not always strangers. In many situations they may already have met them, through their family or social activities, and then use the internet to build rapport with them. Sometimes children don't realise that their beliefs have been shaped by others, and think that the person is their friend, mentor, boyfriend or girlfriend and has their best interests at heart.

1.27 What are the signs I should look out for?

There are a number of signs to be aware of (although a lot of them are quite common among teens). These are some things staff should look out for increased instances of:

- A conviction that their religion, culture or beliefs are under threat and treated unjustly
- A tendency to look for conspiracy theories and distrust of mainstream media
- The need for identity and belonging
- Being secretive about who they've been talking to online and what sites they visit
- Multiple social media profiles or accounts sometimes with variations of names
- Use of known far right or extremist imagery within their social networking profiles
- Switching screens when you come near the phone, tablet or computer
- Possessing items – electronic devices or phones that parents have not provided.
- Becoming emotionally volatile

Reporting

1.28 Online terrorism:

You can report terrorism related content to the police's Counter Terrorism Internet Referral Unit at www.gov.uk/report-terrorism.
Another link http://seeitreportit.org/

1.29 Online Hate speech: Online content which incites hatred on the grounds of race, religion, disability, sexual orientation or gender should be reported to True Vision at www.report-it.org.uk.

In Abingdon Primary School this is achieved through the schools filtering system "Smoothwall" this helps us to detect any warning signs and support vulnerable people whilst using the internet. The smoothwall system offers:

Home Office terrorism blocklist to block terrorist and extremist content per Government guidelines.

- Reporting suite allowing monitoring and reporting on all user access in real time. Detecting warning signs early, preventing them from escalating into more serious issues.
- Custom blockpages can offer channels of support instead of the default blockpage, allowing you to continue the conversation and provide help to vulnerable students or staff.

1.30 Online Child Sexual Exploitation (Online CSE)

(Also refer to the Safeguarding and child protection policy)

Online CSE is a form of sexual abuse where children are sexually exploited in exchange for money, power or status, online CSE can involve many of the similarities with physically CSE but allow offenders to operate under a further guise of secrecy, it can also enable predators to target victims much more easily.

Online CSE can involve humiliating and degrading sexual assaults, in some cases young people are persuaded or forced into exchanging sexual activity for money, drugs, gifts, affection, or status.

Child sexual exploitation is explained more in the schools Safeguarding and Child Protection Policy and outlines that exploitation does not always just involve physical contact and that, webcams, photographs, applications and websites can also be used in the targeting, selection and friendship forming stages of the grooming process.

Some of the following signs may be indicators of online sexual exploitation

- Displaying changes of behaviour or emotional wellbeing
- Leaving the room to check devices more often
- Becoming more secretive about who they are talking to online
- Changing passwords on devices or applications to prevent access
- Unexplained gifts or online items, levels or perks purchased

Online Child Sexual Exploitation (CSE) incidents should be reported in line with Abingdon's Safeguarding and Child Protection Policy.

All Incidents of online CSE should:

- Reported to the schools DSL, who will record details on CPOMS accurately.
- Ascertain if parents are aware of the issue.
- If the child is in immediate risk i.e. they have arranged to meet an online child sex offender the police should be informed immediately.
- Recorded on CPOMS
- Individual incidents could be reported to the Child Exploitation and Online Protection Centre if required and we would support the family in completing this process and complete with parents where required.

http://www.ceop.police.uk using their online report form

- If appropriate inform first contact 01642 728004.

Cyberbullying

1.31 Strategy to deal with cyberbullying, as taken from guidance from Childnet International

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
The school will follow procedures in place to support anyone in the school community affected by cyberbullying.
Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying e.g. telling a trusted adult, Online bully box, Childline Phone number 0800 1111.
Pupils, staff and parents and carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence.
All incidents of cyberbullying reported to the school will be recorded by the school.
The school will follow procedures to investigate incidents or allegations of cyberbullying.
The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's e-safety ethos.
Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

- The bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content

Internet access being suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP

- The parent and carers of pupils being informed

- The police being contacted if a criminal offence is suspected

TELL SOMEONE- We will actively encourage our pupils to speak to their class teacher or school safeguarding officer if they become the victim of bullying, cyberbullying or trolling.
DO NOT REPLY – DO NOT RETALIATE-We will ask children not to reply to the perpetrator, a cyberbully or troll, like a playground bully often wants a reaction and without one this means they will often have less chance of success to cause harm.
BLOCK THE BULLIES- We will advise and offer guidance throughout the year of our pupils to block anyone who is sending them distressing or upsetting messages and advise them to remove the perpetrator from their contacts.

KEEP THE EVIDENCE

The school will make a record of every bullying incident on CPOMS, **we will ask pupils and parents to take screen shots from the device**, unless this consists of content which could be deemed illegal, such as indecent images of children.

1.32 How will we teach children about Bullying/Cyberbullying

There are explicit links and overlaps between for teaching about Cyberbullying/ Digital Safeguarding within computing curriculum, PSHE other curriculum areas and assemblies.

1.33 Resources to deal with Cyberbullying

The school will use as the resource for Bullying these are:
http://www.childnet.com
http://www.childnet.com/ufiles/Cyberbullying-guidance2.pdf

Online Gaming

Lots of our pupils love playing games online. We as a school understand that this is an exciting and interesting environment for children where they can play in real time with people across the world through a computer, games console, tablet or smartphone connected to the internet. Games can offer children a world of adventure to immerse themselves in, but it's important to understand how children can stay safe and what games are appropriate for their age.

1.34 Parents tips regarding Online Gaming- Taken from UK Safer Internet Centre.

- Beware of gaming sites that ask you to reveal personal details or information
- Beware of online bullies/trolls, they also operate in these environments.
- Don't forget that some of the people that you are playing online are strangers.
- Don't arrange to meet people you have met online, keep your online friends…online
- Online gaming is often uncensored and the content may not be suitable for your child's age group
- Pay attention to PEGI ratings when purchasing games, these are an age restriction, not a skill level
- Be careful with subscriptions and purchasing online items, sometimes commercialism is used within these gaming environments.
- Online gaming is known to be habit forming, set a limit on the amount of time your child spend online gaming
- Set up a family agreement for acceptable use
- Online gaming has different risk to other forms of internet use as they often contain elements of social networking, voice over IP, face to face chat and or forums.

1.35 Youth Produced Sexual Imagery - Steps to take when dealing with an incident

The definition of 'youth produced sexual imagery'
There are a number of definitions of youth produced sexual imagery but for the purposes of this advice youth produced sexual imagery is simply defined as digitally produced images or videos generated:

• by children under the age of 18, or
• of children under the age of 18 that are of a sexual nature or are indecent. These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know.

Steps to take in the case of an incident

STEP 1: Disclosure by a pupil

Youth produced sexual imagery disclosures should follow our normal safeguarding practices in lines with the schools safeguarding and child protection policy. If an incident of youth produced sexual imagery has occurred, it is likely the pupil will be very distressed, especially if the image has been circulated widely and further anxiety if they don't know who has shared it, seen it or where it has ended up.
It is also likely that the pupil will need support during the disclosure and after the event. They may even need immediate protection or a referral to social care.
The following questions will help decide upon the best course of action:
• Is the pupil disclosing about themselves receiving an image, sending an image or sharing an image?
• What sort of image is it? Is it potentially illegal or is it inappropriate?

• Is the school's Safeguarding Policy and practices being followed? For example, is the Designated Safeguarding Lead (DSL) on hand and is their advice and support available?

• How widely has the image been shared and is the device in their possession?

• Is it a school device or a personal device?

• Does the child need immediate support and/or protection?

• Are there other pupils/children involved?

• Do they know where the image has ended up?

This situation will need to be handled very sensitively. Whatever the nature of the incident, ensure the school Safeguarding and Child Protection Policy and the Digital Safeguarding Strategy and practices are adhered to.

STEP 2: Searching a device – what are the rules?

In a school-based context, it is highly likely that the image will have been created and potentially shared through mobile devices. It may be that the image is not on one single device: it may be on a website or on a multitude of devices; it may be on either a school-owned or personal device. It is important to establish the location of the image but be aware that this may be distressing for the young person involved, so staff must be conscious of the support they may need.

The revised Education Act 2011, section 94, brought to bear significant new powers and freedoms for teachers and schools. Essentially, the Act gives schools and/or teachers the power to seize and search an electronic device if they think there is good reason for doing so. A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or pornography. The following rules must be adhered to when a device is confiscated and needs to be searched.

- Parents need to be informed as soon as possible.
- The action is in accordance with the school's Safeguarding and Child Protection Policy and the Digital Safeguarding Strategy.
- The search is conducted by the Head Teacher or other nominated safeguarding lead authorised by them.
- The DSL or a deputy is present.
- The search is conducted by a member of the same sex.
- The search is conducted in a private and confidential safe area.
- Types of images and nature of incident need to be considered. If any illegal images of a child are found, you should consider whether to inform the police.
- Aggravated incidents - Any conduct involving, or possibly involving, the knowledge or participation of adults indicates significant harm and should always be referred to the police.
- Aggravated incidents – Any conduct involving children and young people with intent to cause harm, abusive or criminal elements should also be referred to the police
- Aggravated incidents – Any conduct involving children and young people where an image has been sent without the knowledge or will of the pupil should be referred to the police

- Experimental incident are those which could include but are limited to romantic interests, sexual attention seeking, established relationships or where no malice or mal-intent is intended

- Experimental incidents are not always required to be referred to the police, the National Police Chief Council recently produced guidance on dealing with 'experimental' incidents of youth produced sexual imagery to police forces and any incidents reported to police which could be deemed "experimental" will likely be recorded under the polices Outcome 21 code, which means no criminal case will be pursued.

- The reasons for not informing the police recorded on CPOMS

- The Always put the child first. Do not search the device if this will cause additional stress to the child/person whose image has been distributed.

Staff should never:

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the child UNLESS there is clear evidence to suggest that there is an immediate safeguarding issues
- Print out any material for evidence
- Save any material to a schools network
- Move any material from one storage device to another

Always:

- Inform the school's Designated Safeguarding Lead
- Record the incident
- Act in accordance with school Safeguarding Policy and procedures
- Inform relevant colleagues/senior management team about the alleged incident before searching a device
- Inform the pupils parent/guardian

If there is an indecent image of a child on a website or a social networking site, then you should report the image to the site hosting it. If the content includes child sexual abuse imagery, nudity or criminally obscene material the Internet Watch Foundation can be contacted to have this content removed https://www.iwf.org.uk/

Where you feel that the pupil may be at imminent risk of abuse or victim of grooming with intent to meeting a pupil, then you should report these incident directly to CEOP https://www.ceop.police.uk/ceop-report.

This is so that law enforcement can make an assessment, expedite the case with the relevant provider and ensure that appropriate action is taken to safeguard the child.

STEP 3 - What to do and not do with the image.

If the image has been shared across a personal mobile device:

Always:

- Confiscate and secure the device(s)

Never:

• View the image unless there is a clear reason to do so (see section 2)
• Send, share, copy or save the image anywhere
• Allow children to do any of the above

If the image has been shared across a school network, a website or a social network:

Always:

• Block the network to all users and isolate the image

Never:

• Send, share, copy or save the image
• Move the material from one place to another

• View the image outside of the protocols in the school's Safeguarding Policy and procedures.

STEP 4 - Who should deal with the incident?

Often, the disclosure will be made from a child to their class teacher. Whoever the initial disclosure is made to must act in accordance with the school's Safeguarding and Child Protection Policy and the Digital Safeguarding Strategy
They must ensure that the Designated Safeguarding Lead (DSL) or a deputy DSL are involved in dealing with the incident immediately. The DSL should always record the incident using CPOMS.

As described in section 2, there may be instances where the image needs to be viewed and this should be done in accordance with this guidance. The best interests of the child should always come first; if viewing the image is likely to cause additional stress, professionals should make a judgement about whether or not it is appropriate to do so.

STEP 5 - Deciding on a response

There may be a multitude of reasons why a child has engaged in youth produced sexual imagery – it may be a romantic/sexual exploration scenario or it may be due to coercion or grooming. Parents need to be involved in every scenario, unless there is a significant risk to the child.
It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that incidents are consistently recorded. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

Always:

• Act in accordance with the school's Safeguarding and Child Protection Policy

• Store the device securely

• Carry out a risk assessment in relation to the child

• Make a referral to first contact **MACH 01642 130700** if needed

• Contact the police (if appropriate) **101**

• Put the necessary safeguards in place for the child, e.g. they may need counselling support, immediate protection and parents **must** also be informed, unless there is significant reasons for not doing so, these should also be recorded.

• Inform parents and/or carers about the incident and how it is being managed and regularly update them with decisions made.

STEP 6 - Contacting other agencies (making a referral)

If the nature of the incident is high-risk or aggravated, consider contacting your local children's social care team. Depending on the nature of the incident and the response, you may also consider contacting your local police or referring the incident CEOP.www.ceop.police.uk

Reporting and Response to incidents

1.36 Handling complaints

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

1.37 Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child Sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the Internet.

1.38 Useful sites

Child Sexual Exploitation

Child Exploitation and Online Protection
www.ceop.police.uk/safety-centre

Childline
www.childline.org.uk

The Internet Watch Foundation
www.iwf.org.uk

Virtual Global Task Force
www.virtualglobaltaskforce.com

Specific Safeguarding Issues

Cyberbullying, Online CSE, Radicalisation, Inappropriate Content

Childnet
www.childnet.com

Think U Know – Resource Library on CSE and Cyberbullying
www.thinkuknow.co.uk/teachers

Guidance and Resources on Youth produced sexual imagery

www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Childline
www.childline.org.uk

Social Media Guides

INEQE Group H2B Social Media Guides

Free subscription required
https://h2bsafetycentre.com/