DIGITAL RESILIENCE STRATEGY 2017/18

Contents

Section 4
Social Networking

Section 5
Mobile Devices

Section 6
Specific safeguarding issues

Section 7
Cyberbullying and Trolling

Section 8
Online Gaming

Section 9
Sexting

Section 10

DIGITAL RESILIENCE STRATEGY 2017/18

Section 1
Strategy Overview

1.1 Strategy Statement

This strategy is designed to be a simple to understand and comprehensive resource in regulating all digital activity in Newport Primary School. It will provide a clear understanding of appropriate behaviours and access to digital devices that members of the school community can use as a reference for conduct, contact and content online both inside and outside of the school hours.

'Digital Safeguarding and Resilience' is a whole-school issue and responsibility. In addition, there is a 'duty of care' for any persons working with children or members of the school community to educate on the risks and responsibilities associated with living in a 'digital world'. 'Digital safeguarding' falls under this duty and this strategy aims to highlight this duty.

In the 21st Century, Newport Primary School recognises that ICT and the internet are necessary and fantastic tools for learning. Communication technology can be used in the school to enhance the curriculum, challenge students, raise educational standards and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the safe use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice excellent safeguarding of our pupils.

Digital Resilience is the term used throughout this document in replacement of the outdated and overused term of 'E-Safety'

This updated term takes into account the changes that have occurred in the previous 10 years around technology use. Within these changes have arisen many benefits but have also brought with them many additional risks for our children. It is now a common daily activity for children to use technology and come into contact with a complete stranger whether that be from watching and commenting on their favourite You Tube video, using a chat application or speaking to someone directly on a games console using Voice-over-IP. Given the frequency of these activities, we can therefore no longer look at internet safety matters as a separate thing when it concerns the safeguarding of our children and they should be dealt with and educated in the same way as every day safeguarding matters.

Digital Resilience covers the internet but it also covers mobile phones and other electronic communications technologies including tablets and gaming consoles, which many of our children use. It is important that all members of the school community are aware of the dangers of using internet enabled devices and how they should conduct themselves online both inside and out of school hours. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential.

Our school's strategy for digital safeguarding consists of varying elements consisting of guidance for internet access, computer, tablet and device use and the role of our computing curriculum in teaching children to be digitally resilient. It covers specific contemporary safeguarding matters such as cyberbullying, radicalisation and sexting and draws on guidance from

- Department for Education, Keeping Children Safe in Education 2016
- The Education Act 2011
- Counter-Terrorism and Security Act 2015
- Prevent Duty Guidance 2015
- UK Council for Child Internet Safety (UKCCIS) Sexting for Schools and Colleges Guidance
- Ofsted Guidance on Dealing and Tackling Bullying 2012
- Computer misuse act 1990
- Current advice and best practice from varying online charities including Childline and Internet Matters.
- House of Lords Report, Growing up with the Internet, 2017
- Children's Commissioner Report, Growing up Digital, 2017

It purposely links closely to the schools policies on safeguarding and child protection, preventing radicalisation and bullying.

This strategy has been devised by a team consisting of the Head Teacher, Deputy-Head Teacher, safeguarding leads, and designated specialist representative from local authority. It will be reviewed on a yearly basis and it has been agreed by the senior management and approved by governors.

1.2 Digital Resilience and Newport Primary School

With technology developing at such a tremendous pace, our school realises the importance of our pupils to be equipped from an early age to engage safely and resiliently with technology, the internet and its content.

As described in a recent Young Minds research paper Digital Resilience is a term given to "the social and emotional literacy and digital competency to positively respond to and deal with any risks they (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 w**hat 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

Research data from a recent Mumsnet survey showed that 73% of parents are 'concerned about their children accessing inappropriate materials online' and 61% feared that social media was 'an overwhelming distraction from other activities'.

We want to promote the message to our school community that they make the online world a force for good; a message that equips our pupils with what it means to be a 'good digital citizen'. We also aim to help our pupils to become digitally independent and confident in their choices so they minimise the risk of a mistake happening when interacting with technology or online in the first place.

1.3 Key Personnel

Position	Key responsibilities
Head Teacher and Governors	• Ensure that the Digital Resilience Strategy is implemented and compliance monitored. • Ensure that the appropriate roles (see this section) 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 Leads (DSL) Patricia McGill Louise Hill	• The Designated Safeguarding Leads (DSL) will be the first point of contact with any concerns with regards to digital Safeguarding; they will assess the concern and take the appropriate action needed. • DSL will ensure that all staff are familiar with and adhere to the schools Safeguarding Policy. • Responsible for digital safeguarding developments in the school and sharing of practice with staff, parents and the wider school community. • Will be in receipt of current training on the latest guidance and procedures.

	- Main contact for the Local Authority Digital Safeguarding networks. - All digital safeguarding incidents within the school need to be reported to DSL. - Keep log of incidents on CPOMS. Make decisions (with Head Teacher) about how to deal with any reported incidents.
Computing Co-ordinator - Patricia McGill (Current Head Teacher)	- Ensure up-to-date with latest developments and issues of concern, publicising these appropriately to staff, students and parents. - Be in receipt of all digital safeguarding concerns. - Keep logs of any reported incidents on CPOMS and actions taken to resolve these. - Have appropriate training and skills for this level of post. - Hold CEOP 'Think You Know' trained status
All Staff	- All school staff with subject and management roles have a duty to incorporate digital safeguarding principles in their area of responsibility. - 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 a DSL for recording on CPOMS. - All staff will undertake annual 'digital safeguarding' training with local authority.

1.4 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.

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.

Section 2
ICT and Newport Primary School

2.1 Making use of ICT and the internet in the School

The internet is used in Newport Primary School to raise educational standards, promote pupil achievement, support the professional work of staff and to enhance the schools management functions.

Our computing curriculum aims to enrich, modernise and support all aspects of our school's curriculum. Pupils learning should be made more rewarding and inspirational by using ICT. Pupil's confidence and progress in their computing skills is essential for them to maximise their learning in the curriculum and to prepare them for the challenge of a rapidly developing and changing technological world in both education and business.

We want to equip all of our pupils with all of the necessary computing skills that they will need in order to enable them to progress confidently, and more importantly, safely into further learning environments and employment when they leave the school.

2.2 Benefits of ICT and the Internet

At Newport Primary School, ICT and access to the Internet are used in a range of ways including:

Access to world-wide educational resources including museums and art galleries.

- Inclusion in government initiatives such as the 'Think You Know' resources.
- Information and cultural exchanges between pupils world-wide.
- Cultural, social and leisure use in libraries, youth clubs and at home.
- Discussion with experts in many fields for pupils and staff.
- Staff professional development - access to educational materials and good curriculum practice.
- Access of You Tube videos to assist in learning.
- Collaboration and communication with the advisory and support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with the LA and DfE.
- Electronic capture and monitoring of relevant school//pupil data in the form of management information (MI).

2.3 Objectives of the computing curriculum

- Ensure a broad and balanced computing curriculum is provided for all children regardless of ethnic origin, gender, class, aptitude or disability.
- Meet the national curriculum requirements for computing across all key stages.

- Embed computing across a curriculum that acknowledges its contribution to learning in all other subjects.
- Equip pupils with a progression of computing skills that they can apply both in and out of school.
- Support all staff to make effective use of ICT at a professional level.
- For computing to have a positive impact on pupils' creativity, motivation, independence and collaboration, behavior and attitudes.
- Provide our pupils with an enjoyable experience of computers so that they will develop a deep and lasting interest and may be motivated to use them further.
- For pupils to use computers in experimental, imaginative, exploratory ways. This will include regular opportunities to engage with computer programming.
- Ensure that staff and pupils understand the capabilities, advantages, risks and limitations of ICT and consider the implications of its development for society.
- Make effective use of computers to transform teaching and learning providing opportunities that would otherwise not be possible.
- Facilitate electronic communication between home and school.
- Ensure the safety and well-being of our pupils.
- Teach computing in line with the principles of our teaching and learning policy.
- Ensure computing resources are relevant and sufficient.

2.4 Planning the computing curriculum

Newport Primary School believes that all pupils should have access to a broad, rich and creative curriculum that reflects their range of experience and is set at an appropriate level that offers both challenge and support.

Our computing curriculum aims to:

- Equip our pupils to be good digital citizens.
- Be 'real' and relevant to their interests and experiences.
- Engage, interest children and offer opportunities to investigate, problem solve and communicate in different ways.
- Be progressive, building upon prior learning.
- Be focused upon developing key skills across subjects.
- Be flexible to meet the changing needs and interests of all learners.

2.5 Assessment

The progress of classes and year groups in ICT is evaluated by:

- Monitoring attainment by observation of teaching and learning in the ICT suite and in other curriculum areas.
- Monitoring coverage through completion of the skills based planning framework.
- The progress of individual children's attainment is monitored by the class teacher against the ICT skills as defined by the National Curriculum.

2.6 Responsibilities

The school's teaching should be made more creative and effective by using computers which provide innovative experiences that would either be less inspiring or impossible without them.

The Head Teacher & Governors will:

- Monitor the implementation of the Digital Resilience Strategy.
- Ensure there is a long term plan that details coverage and progression.
- Oversee teaching, learning and standards in computing.

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 relevant CPD for staff.
- Manage the computing resources in the school.
- Manage the work of the school's technician currently commissioned to One IT Services and Solutions (One ITSS).
- 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 the Digital Resilience Strategy.

Teachers will:

- Use the long term plan for computing to plan opportunities for all pupils to develop a broad range of appropriate computing skills.
- Plan opportunities for the relevant and creative use of ICT across the curriculum on an ongoing basis.
- Plan for differentiation so that all pupils develop computing skills, taking into account the individual needs of children. This includes SEN, higher ability children and those with less access to computers at home.
- Ensure the appropriate time is allocated to discrete teaching of computing and computer programming.
- Report pupil's achievement in ICT in the annual report to parents.
- Follow health and safety guidelines and the Digital Resilience Strategy.

All staff will:

- Ensure all adults and children handle and use ICT equipment in an appropriate way.
- Be equipped and continually updated with computing skills and resources that enable them to feel confident in using ICT effectively in their teaching and wider professional role.
- Follow health and safety guidelines and sign the 'Acceptable Use of ICT agreement'.

2.7 What pupils will learn about computing:

Key Stage 1
Be taught to:

- Understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions.
- Create and debug simple programs.
- Use logical reasoning to predict the behaviour of simple programs.
- Use technology purposefully to create, organise, store, manipulate and retrieve digital content.
- Recognise common uses of information technology beyond school.
- Use technology safely and respectfully and keep personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2
Be taught to:

- Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- Use sequence, selection, and repetition in programs; work with variables and various forms of input and output.
- Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs.
- Understand computer networks including the internet; how they can provide multiple services, such as the internet; and the opportunities they offer for communication and collaboration.
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

- Use technology safely, respectfully and responsibly; recognise acceptable/ behaviour; identify a range of ways to report concerns about content and contact.

2.8 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 via taught lessons.
- Posters and publicity materials promoting good digital safeguarding practices will be displayed next to all computers within classrooms and in a prominent place within the ICT suite, so that all users can see them.
- 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 frequently reminded of being safe online and being a good digital citizen.

2.9 How will we teach about Digital Safeguarding in PSHE 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 the schools PSHE programme of study in relation to Digital Safeguarding.

Newport Primary School takes into consideration the findings from the Children's Commissioner Report 'Growing up digital' and we aim to ensure that our teaching of the computing curriculum is not done in isolation and does not only concentrate on things such as coding, algorithms and processes; but also teaches the social elements of life online including how to critique content, recognise fake news, assess body image, how to control own online activity and what to do when this becomes problematic.

2.10 How pupils will be taught to assess Internet content

Pupils in school are unlikely to see inappropriate content in books due to selection by publishers and teachers. This level of control is not so straightforward with the internet and online based materials. Therefore, teaching should be widened to incorporate internet content issues, for instance the value and credibility of web materials such as in relationship to other media. The tendency to use the web when better information may be obtained from books will need to be consistently challenged.

Teaching will be age-appropriate, depending upon the age of stage of the child and may include:

- Pupils will be taught ways to validate information before accepting that it is necessarily true, this could include recognising fake news.
- Pupils will be taught to acknowledge the source of information and observe copyright when using internet material for their own use.
- Pupils will be made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

2.11 Managing emerging technologies

Emerging technologies will be examined for educational benefits and risk assessment will be carried out before use in school is allowed.

2.12 Acceptable use

All ICT use in school should follow these guidelines and staff will be expected to be diligent and use their professional judgment, in relation to their own conduct and the conduct of pupils as appropriate:

- 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 lines with the schools Bullying and Behaviour Polices.
- Staff inappropriate internet or ICT use will be dealt with in line with the schools local authorities (LA) disciplinary procedures.
- All staff will have access to this Digital Resilience Strategy and reminded of its importance.
- Staff will be made aware that internet traffic is monitored or inappropriate usage and relevant action will be taken as necessary (see section 3).
- Discretion and professional conduct is essential.
- Staff must always use a child friendly safe search engine when accessing the internet with pupils.
- YouTube use within the school on all devices is set at restricted use, this helps screen out any potentially mature content.

2.13 Resources

ICT resources are available in every classroom including:

- Every class having a main computer.

- Each classroom/teaching area is equipped with an interactive whiteboard and projector.
- All classes have access to a visualiser.
- Use of Apple IPads are available.
- Laptops are available for both pupils and staff.
- IT Suite is fully equipped with touch-screen computers and Apple IPads.

2.14 Special Education Needs

Support for children who have SEND in ICT is augmented by the Computing Co-ordinator, who, in conjunction with class teachers, provide individual education programs and resources where and when appropriate.

2.15 Handling complaints

- The Head Teacher will deal with all complaints of internet misuse.
- Any complaint about staff must be referred to the Head Teacher who will decide on an appropriate course of action.
- Any issue that cannot be resolved by the Head Teacher or the senior leadership team will be referred to the Chair of the board of governors.
- Complaints of safeguarding or child protection must be dealt with in accordance with the schools Safeguarding and Child Protection policy.

2.17 Staff and pupil consultation about the internet

- It is very important that staff are confident in the use of the internet and consider that the school ‘Acceptable use agreements’ and the Digital Resilience Strategy are appropriate and fit for purpose.
- Staff should be given opportunities to discuss any issues and develop appropriate resilience and teaching strategies. It would be unreasonable if staff, particularly supply staff, were asked to take charge of an internet activity without training. Reassurance and discussion may be required.

Section 3
Management of School Information Technology (ICT) Systems

3.1 The maintenance of security of the ICT systems

The internet is a connection to the outside world; lack of security within the schools ICT system could compromise systems performance, threaten security of the schools ICT system or cause harm to the entire network.

The ICT systems in Newport Primary School are managed by One IT Services and Solutions, who will provide IT support to Newport Primary School 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 schools ICT strategy by ensuring the development and delivery of quality ICT services. These services will include

- Broadband provision.
- MIS System training.
- Website hosting.
- Help and Support with Microsoft Office Products.
- 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 Newport Primary School pupil data is stored securely on the schools secure network.
- Management and support of the schools anti-virus protection, the schools uses ESET Endpoint Antivirus - NOD32.
- This software will be installed on all schools devices and updated automatically each time an update is released.
- Ensure the use of e-mail and attachments will be monitored closely.

3.2 Data Management

The School will ensure that:

- Sensitive pupil information is only accessed by secure means.
- Any school documents (e.g. planning) can only be taken off site if stored on an encrypted memory stick.
- Any sensitive data sent by e-mail should only be sent to secure e-mail address and/or password protected.
- Personal data is not sent over the internet from school, unless sent to secure e-mail or file server.

3.3 Filtering and Monitoring Systems

To support the prevention of accessing any unsuitable, age inappropriate, illegal, extremist or radical material on the schools ICT, the school commissions One IT Services and Solutions (One ITSS) to manage and monitor its filtering systems. The services offered combine management of classroom ICT, network management and desktop management.

The technical strategies developed with One ITSS restrict access to inappropriate material. Material can fall into several overlapping types and there are categories that are blocked as standard (sometimes referred to as filtering).

Blocking strategies are in place to remove access to a list of unsuitable sites or newsgroups completely. Maintenance of the blocking list is a major task as new sites appear every day. One ITSS will manage the blocking and unblocking of websites on behalf of school and keep appropriate filtering logs and report where required.

Filtering examines the content of web pages or e-mail messages for unsuitable words. Filtering will be applied based upon current national guidelines for schools.

Blocking and/or filtering is performed by software called Smoothwall.

The school has invested through One IT Services in Smoothwall software that does the following:

- Prevents access to unsuitable sites filtered by key words including multi-lingual filtering.
- Prevents access to proxy sites.
- Requires administrative rights to install new software.
- Enforces the schools 'Acceptable use policy'.
- Creates key word libraries for real-time detection.
- Determines potential risk through key word glossaries with explanations.
- Captures time stamped screen shots of violations.

If staff or pupils discover an unsuitable site, it must be reported to the schools DSL.

3.4 Filtering - Preventing Radicalisation – under section 29 Counter-Terrorism and Security Act 2015

The volume of terrorist and extremist content online is a growing concern, with an 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 that those under our care are being prevented from 'being drawn into terrorism' and 'non-violent extremism'.

In Newport 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, as 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 designated staff to take appropriate action involving

conversation with identified individuals in order to provide help to vulnerable students or staff.

3.5 Ensuring safe internet access

The internet is a global computer network providing a variety of information and communication facilities. It is available to anyone, and allows access for people to view, search, or publish information on almost any topic. Access to appropriate information should be encouraged but internet access must be safe for all members of the school community from youngest pupil, to teacher and administrative staff. Pupils will generally need protected access to the internet.

Pupils will be informed that internet use will be supervised and monitored. The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems in place to protect pupils are continually reviewed and, where necessary, improved.

Senior leadership team and designated safeguarding lead will ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice.

- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to One IT Solutions by the computing coordinator.
- Any material that the school suspects is illegal will be referred to the Internet Watch Foundation.
- Where minority languages are involved, appropriate measures will be taken to ensure the processes to protect pupils are adequate.

3.6 The assessment of risk when using the internet in school

The school will address the issue that it is difficult to completely remove every risk that pupils might access unsuitable materials via the school system, in common with other media such as magazines, books and video. Some material available via the internet is unsuitable for pupils even with filters from Smoothwall in place.

The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material, including the use of filtering software, Smoothwall.

However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that unsuitable material will never appear on a computer or device. The school therefore cannot accept liability for the material accessed, or any consequences thereof.

Matters to consider on internet access:

- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed.
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken.
- The Head Teacher will ensure that the Digital Resilience Strategy is implemented effectively.

3.7 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. It can also 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, therefore ground rules are 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 considered inappropriate on school websites. While any risks might be small, the parents' perception of risk has been taken into account.

- 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 website should be the school address, e-mail and telephone number. Personal information or individual e-mail identities will not be published.
- Photographs will be selected carefully and 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 website, particularly alongside photographs.
- Written permission and consent from parents will be sought before photographs of pupils are published on the school website.

3.8 The management of e-mail

E-mail is an essential means of communication within education. The school encourages the ownership of individual e-mail accounts for both teachers and pupils, but care needs to be taken that the implications for the school and for the pupil are appreciated. Once e-mail is available, it is difficult to control its content, nevertheless e-mail content should not be considered private.

- Pupils from Key Stage 2 may have e-mail, but will be taught appropriate use.
- One ICT Services and Solutions will create and maintain the e-mail system for staff and pupils that is accessible from home and external locations with a large mail box and shared school calendar.
- The e-mail solution will be Office 365 and will be accessible on devices that operate either Apple or Windows software.

Software is in place to restrict incoming and outgoing e-mail to a list of approved establishments as the filtering of e-mail for unsuitable content and viruses that could compromise the school network is possible.

3.9 E-mail code of conduct

Staff

- Individual school e-mail accounts must only be used for educational purposes.
- The forwarding of chain e-mails will be banned, as will the use of chat applications, the school has its own internal messaging alert system called ‘Link’ which is the only chat application that will be allowed to be used in school.
- Staff should use official school e-mail accounts to communicate with parents or external organisations. Personal e-mail accounts should not be used for this purpose.
- E-mails sent from the school should be professionally and carefully written.
- Staff must inform the Head Teacher or senior leadership team if they receive any offensive, threatening or unsuitable e-mails

Pupils

- Pupils should tell a member of staff if they receive any inappropriate e-mails.
- In line with the Digital Resilience Strategy, pupils should not send any offensive, threatening or unsuitable e-mails to any other e-mail account.
- In line with the Digital Resilience Strategy, students should not reveal any personal information over e-mail, or arrange to meet up with anyone they have met online.
- As part of the computing curriculum, pupils will be taught to identify spam, phishing and viruses and that these can cause harm to the schools network.
- Student e-mail will have inappropriate words filtered and the school will be informed if a student’s account triggers an inappropriate e-mail violation alert.

- Pupils currently send internal e-mail messages as part of planned lessons.

3.10 The authorisation of internet access

Newport Primary School grants internet access to all staff and all pupils. Parental permission is 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, sexting and cyberbullying and who to report to if they are concerned by anything they have seen or heard on the internet.

The following points should also be noted:

- Connecting school ICT equipment to home networks IS PERMITTED, both via wireless network (Wi-fi) and wired via Ethernet cable.
- Staff must not connect to internet by installing proprietary software e.g. service provider software on a CD or download.
- Staff must ensure their home wireless network connection has the appropriate security encryption of at least WAP2 (if you have to enter a password to access your home Wi-fi, then it is likely the system is already in place).

Section 4
Social networking, social media and personal publishing

4.1 What is Social Networking?

We recognise that social media and personal publishing sites may have benefits for learning; however both staff and pupils should be aware of how they present themselves in the online context. The current use of school equipment or network for the use of social media is prohibited, with the exception of You Tube which we recognise has many benefits for both pupil and professional learning, although this use is restricted.

Social networking applications and personal publishing tools could include, but are not limited to:

- Social Networking (E.g. Facebook, Instagram, Snapchat).
- Messenger Apps (E.g. Facebook Messenger, Whatsapp, KIK, Viber).
- Video chat applications (E.g Skype, Omeagle, Yellow).
- Media sharing services (E.g. Musical.ly, You Tube, Vines).
- Micro-Blogging Applications (E.g. Twitter).
- Online discussion forums (E.g. Reddit, 4 Chan, IGN).
- Blogs (E.g. Blogger, Live Journal, Xanga).

Social networking sites, bulletin boards, forums, video conferencing, chat rooms and instant messaging applications are all strictly prohibited on school device or network.

Some of these online environments can be main sources of inappropriate and harmful behaviours, where the most vulnerable can be contacted by a potentially dangerous person.

4.2 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.

Newport Primary 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 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 of getting something removed once it is in the public domain.

In the context of social media, pupils will be taught about:

- Contact
- Conduct
- Content
- Commercialism

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
- How terms and conditions work on downloading certain applications
- How to use social networking sites in safe and productive ways
- How to use the schools 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

4.3 The pupil Acceptable Use Agreement (for pupils and staff)

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the Digital Resilience Strategy, its importance explained and will sign to say they understand its contents.
- Parents' attention will be drawn to the strategy in newsletters, the school brochure and on the school website.
- A module on responsible internet use including social media will be included in the computing curriculum scheme of work, covering both school and home use.

4.4 Enlisting parental support for the use of the internet

- Internet use in pupils' homes is increasing rapidly.
- Pupils may have unsupervised and unrestricted access to the internet, parents may need to be made aware of the dangers of this to ensure they put appropriate controls in place.
- The school may be able to help parents plan appropriate, supervised use of the internet at home through the use of family agreements.
- A careful balance between informing and alarming parents will be maintained.

- Demonstrations and practical IT sessions for parents may be organised to encourage a partnership approach.
- Joint home/school guidelines on issues such as safe internet use will be established;
- Suitable educational and leisure activities that make responsible use of the internet will be developed with parents.
- A stock of relevant posters and information leaflets from organisations such as CEOP and Childnet will be available.
- Annual CEOP parental workshop will be provided to all parents.

4.5 Staff Social Networking

This section sets out the schools recommendations and requirements for the use of social networking by our staff members. In doing so Newport Primary School seeks to achieve an appropriate balance in the use of social networking by staff as private individuals, but also as employees and educators, with professional reputations and careers to maintain, and legislative requirements to adhere to.

Newport Primary School does not wish to discourage staff from using such sites and applications in their own personal time, we do however aim to protect staff from the pitfalls of in-appropriate use, and we do expect certain standards of conduct to be observed in order to protect the school reputation and prevent from bringing the school into disrepute.

Accessing social networking sites in work time, using school ICT internet connections is strictly forbidden, using the schools ICT equipment to access social networking either at home or at the school is also strictly prohibited.

4.6 Eligibility

This guidance therefore largely relates to the use of social networking applications by the school staff in their own personal time, using their own ICT equipment or devices.

Newport Primary School is committed to safeguarding and promoting the welfare of our children and young people and expects all staff, volunteers and visitors to the school to share this commitment.

The term ‘staff’ covers all employees of the school, including casual staff and agency employees. Where individuals from partner organisations are involved in acting on behalf of the school, they will also be expected to comply with this guidance.

4.7 Exceptions

Staff will be required to sign the Staff ‘Acceptable use policy’ agreement

Pupil use of these sites using the school network is covered in the pupil ‘Acceptable use policy’ agreement.

4.8 Responsibility & Accountability

Head Teacher & Senior leadership team will:

- Ensure that all existing and new staff are familiar with the schools Digital Resilience Strategy and its guidance and code of conduct when using social networking and ICT.
- Provide opportunities to discuss appropriate social networking use by staff on a regular basis and ensure that any queries are raised to resolve swiftly.
- Ensure that any allegations raised in respect of accessing social networking sites are investigated promptly and appropriately, in accordance with the schools disciplinary procedure and code of conduct and disciplinary rules.

Staff:

- Should ensure that they are familiar with the contents of the Digital Resilience Strategy and the schools expected standards and guidance on the use of ICT, as stated in the strategy.
- Should raise any queries or areas of concern they have relating to the use of social networking and interpretation of this strategy with their line manager in the first instance.
- Must comply with this strategy where specific activities and conduct are prohibited.

Human Resources will:

- Advise and support the Head Teacher on the application of the policy.

Governors:

- Will review this strategy and its application on an annual basis.
- Should ensure that their own conduct is in line with that expected of staff, as outlined in this strategy.

4. 9 Recommendations and requirements when using social networking sites

Working in an educational setting with children, staff have a professional image to uphold, how individuals conduct themselves online, helps to determine this image. The following points provide staff with recommendations and requirements when staff use social networking sites.

4.10 Friends/Befriending

One of the functions of social networks is the ability to friend request others; this creates a group of individuals who share personal views and/or interests. The school prohibits staff from accepting invitations from pupils, or pupil’s family members and friends.

Staff must also not initiate any contact or online friend requests with pupils or pupil's family members or friends under any circumstances.

Staff who maintain social networking friendships with work colleagues are required to adhere to the requirements below relating to content of interactions.

4.11 Content of interactions

Staff should 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 schools policies for 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, discriminatory; or

Staff must not post comments or entries onto social networking social networking sites which could be deemed, or interpreted, as confidential or which could be deemed as derogatory, defamatory or discriminatory. They should not post comments or entries onto social networking sites relation to pupils or their families in a school context.

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.

Staff must not download copyrighted or 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 or 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.

4.12 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 publically 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 those people they have allowed permission to access their social media account.

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 a pupil, or a group of pupils, has made inappropriate, insulting, threatening or derogatory comments about them, or other staff on a social networking application or site; then they must report this to the Head Teacher or Senior leadership team so that the appropriate processes can be implemented.

4.13 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 (GDPR regulations also to be implemented in May 2018), 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.

4.14 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 which 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.

4.15 Social Networking and Preventing Radicalisation

(This section has been devised in consultation with Andrew Shippey, Community Safety Officer, PREVENT Lead – Middlesbrough Council)

4.16 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; this is due to the fact that it is a worldwide medium, available 24 hours per day, every day, that readily allows people to find and meet people, who may share/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.

4.17 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.

4.18 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/social media platforms 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.

4.19 What are the signs to look out for?

There are a number of signs to be aware of (although a lot of them are quite common among teenagers). 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 such as electronic devices or phones that parents have not provided.
- Becoming emotionally volatile.

4.20 Reporting

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

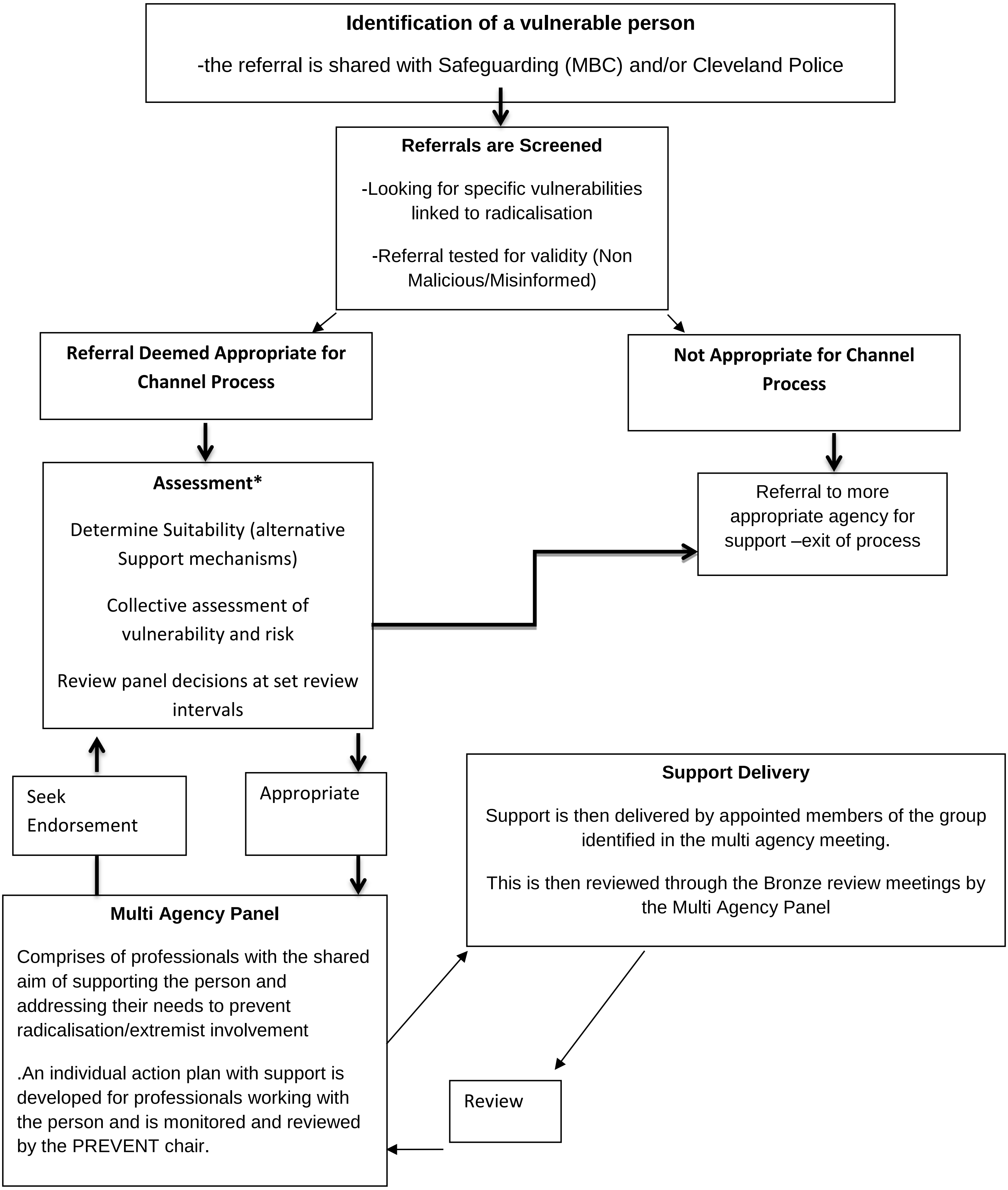
Online Hate speech: Online content which incites hatred on the grounds of race, religion, disability, sexual orientation or gender should be reported to True Vision at www.report-it.org.uk.

4.21 Channel Process

The channel process can be used be any person who suspects/has concerns that a person may be becoming radicalised, and is a process by which that person can be supported/managed depending upon the decisions made within the process.

*Assessment maybe completed based on initial referral and systems interrogation of schools/safeguarding/police and other systems available prior to formal Channel Vulnerability Assessment made with the individual by professional.

A flowchart describing the process that will be followed in order to make and assessment is on the following page.



Identification of a vulnerable person

-the referral is shared with Safeguarding (MBC) and/or Cleveland Police

Referrals are Screened

-Looking for specific vulnerabilities linked to radicalisation

-Referral tested for validity (Non Malicious/Misinformed)

Referral Deemed Appropriate for Channel Process

Not Appropriate for Channel Process

Assessment*

Determine Suitability (alternative Support mechanisms)

Collective assessment of vulnerability and risk

Review panel decisions at set review intervals

Referral to more appropriate agency for support –exit of process

Seek Endorsement

Appropriate

Support Delivery

Support is then delivered by appointed members of the group identified in the multi agency meeting.

This is then reviewed through the Bronze review meetings by the Multi Agency Panel

Multi Agency Panel

Comprises of professionals with the shared aim of supporting the person and addressing their needs to prevent radicalisation/extremist involvement

.An individual action plan with support is developed for professionals working with the person and is monitored and reviewed by the PREVENT chair.

Review

5.0 Mobile devices: Staff, pupils and parents

5.1 Staff

- Staff must not use mobiles phones during ‘school time’. School time is defined as time in class. Staff are permitted to use their devices in staff rooms.
- Staff are not permitted to take photos or videos of students on personal devices, if photos or videos are being taken for curriculum or professional use then school devices (i.e. Ipad, digital camera) should be used.
- Mobile devices should be switched to silent during school hours.

5.2 Pupils

Pupils are not permitted, under any circumstances, 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.

5.3 Parents – ‘Greet your child with a smile, not a phone’

The school will encourage a new policy for parents to ‘Greet your child with a smile not a phone’ when collecting children at the end of the school day, the school will display visual prompts around the school to remind parents of this policy.

Section 6
Specific Digital Safeguarding issues

6.1 Staff Training

- All staff should have an awareness of all safeguarding issues as outlined in the schools ‘Safeguarding and Child Protection Policy’.
- All staff will be trained in the schools strategy for Digital Resilience including annual training, annual curriculum expectations training and introductory briefing from CEOP trained professional on digital safeguarding issues.
- Newport are a members of the Middlesbrough Digital Safeguarding Networking Group
- Newport Primary School will have at least one specialised trained staff member trained to NCA, CEOP - Think U Know trainer level.

Staff will be aware of both historic and contemporary safeguarding issues and in addition staff will also be made aware of specific digital safeguarding issues and the issues which can manifest via peer on peer abuse. These could include, but are not limited to, bullying (including particularly cyberbullying) relationship abuse and youth produced sexual imagery (sexting).

6.2 Peer on Peer Abuse

Staff recognise that children are capable of abusing their peers at any age. We aim to minimise the risk of peer on peer abuse, this is covered explicitly within our ‘Bullying and Behaviour Policy' which sets out how allegations of peer on peer abuse will be investigated and dealt with and how victims will be supported.

6.3 Online Child Sexual Exploitation (Online CSE)

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 physical CSE but allows 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, but also 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 incidents should be reported in line with Newport Primary School Safeguarding and Child Protection Policy.

All Incidents of online CSE should:

- Be reported to the schools Safeguarding Officer, 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.
- Be 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, using the link http://www.ceop.police.uk to access the online report form.
- If appropriate, inform first contact 01642 728004.

Section 7
Cyberbullying and trolling

Cyberbullying and trolling, as with any other form of bullying, is taken very seriously by Newport Primary School. It is not tolerated under any circumstances, nor ever passed off as 'banter' or 'part of growing up' and all incidents will be investigated in line with the schools Bullying and Behaviour Policies.

Research highlights an increase in the use of social media by primary school children, with evidence showing 44% of six year olds are going online, unsupervised in their bedroom with 26% using social media apps (Internet Matters, September 2016).

Almost a quarter (21%) of children aged 8 to 11 will have been deliberately targeted, threatened or humiliated by an individual or by a group through the use of a mobile phone or the internet (Beatbullying, Virtual Violence, 2012).

Childline published the top three concerns young people contacted them for in 2015/16 for counselling sessions as being low self esteem/unhappiness, family relationships and bullying/online bullying (Childline, Annual Report, 2015/16).

Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the schools 'Bullying and Behaviour policies'.

The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not dare do or say in person due to the disconnection from seeking the emotional effects their words or online behaviour is having. The online world also enables others to masquerade behind fake profiles who will then use these to indiscriminately target, humiliate and abuse individuals online this is sometimes referred to as "trolling".

It is made very clear to all members of Newport Primary School community what is expected of them in terms of respecting their peers, members of the public and staff; any intentional breach of this will result in disciplinary action in line with the schools policies.

7.1 Types of Cyberbullying

Threats and Intimidation

- Threats can include violence, including sexual violence, or threats to disclose information about someone that may harm them. For example, to 'out' someone based on their gender identity when they may not feel ready for this.

Harassment or Stalking

- Repeatedly sending unwanted text or instant messages, or making phone calls (including silent calls).

- Using a public forum such as social networking sites, groups or message boards to post defamatory comments.
- Harassing someone by tracking their activities online.
- Doxing (posting or sharing personal information about someone online without their permission).

Ostracising/Peer Rejection/Exclusion

- Setting up closed groups or chats which can be used purposely to exclude others or ridicule them within it.
- Excluding others from online activities.

Identity theft, unauthorised access and impersonation

- Obtaining someone's access to their social media account.
- Cloning social media accounts for the purpose to cause harm.
- Unauthorised use of someones photographs for social media sites.

Publically posting, sending or forwarding personal or private information or images

- Deliberate sharing of private content to embarrass or humiliate.
- Taking photos under cubicles or in changing rooms.
- Creating, possessing, copying or distributing indecent images of children under the age of 18 (Offence).
- Sharing private indecent sexual images of adults with intent to cause distress (revenge porn) (Offence).

7.2 Newport Primary Schools approach to all forms of bullying

In line with the schools Anti-bullying policy, the schools promotes a caring and supportive environment. We are seeking to develop the whole child socially, intellectually, physically and emotionally. We have a range of approaches to reinforce good behaviour within the school. We are continually developing approaches to encourage good citizenship for all our pupils, including the spiritual, moral and social elements.

Opportunities for children to explore difficulties are built in to curriculum time and the structure of the school allows pupils to speak to staff directly. Pupils are actively encouraged to share their feelings, concerns and worries with their parents and carers, in the knowledge that open communication between home and school can help combat bullying. Pupils are also encouraged to share their concerns with other pupils.

Newport Primary School is a **telling** school; this means anyone who is aware of any type of bullying that is taking place is expected to tell a member of staff immediately.

7.3 Spotting the signs of Cyberbullying

Given the nature of cyberbullying it can be less obvious than physical bullying, some signs could include:

- Stopping using their electronic devices suddenly or unexpectedly.
- Becoming particularly secretive or private about what they are doing online.
- Seeming nervous or jumpy when using their devices, or becoming obsessive about being constantly online.
- Any changes in behaviour such as becoming sad, withdrawn, angry or lashing out.
- Reluctance to go to school or take part in usual social activities.
- Unexplained physical symptoms such as headaches, stomach upsets.
- Avoiding discussions about what they're doing online or who they're talking to.

7.4 School strategy on dealing with Cyberbullying, as taken from guidance from Childnet International

TELL SOMEONE
Newport Primary School recognises that there is no substitute for open discussion on this subject; we will hold open discussions during computing and PSHE lessons and circle time and we will promote an emotionally supportive environment, attitude and ethos for our pupils to share their concerns around this subject both in the real world and the online context.
We are a **telling** school and 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, a cyber-bully often wants a reaction and without one this means they will often have less chance of success to cause harm. Often, a reaction from a victim gives the bully more power and only encourages them to do it more.

BLOCK THE BULLIES
Social media sites such as Facebook, Instagram and Snapchat have built in tools to allow users to block anyone who is causing them problems/distress online. 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 grabs from the device**, unless this consists of content which could be deemed illegal, such as indecent images of children. We will

promote to our pupils that the more evidence they can gather, the easier it will be to resolve the situation.

7.5 Dealing with Cyberbullying

If an allegation of peer on peer abuse or bullying does come up, the school will:

- Take it extremely seriously and make parents, governors, pupils and staff aware of this message.
- Provide a caring and safe environment.
- Listen to the victim.
- Act as quickly as possible to establish the facts. (It may be necessary to examine schools systems and logs if they have been used or contact the service provider in order to identify the perpetrator).
- Inform parents and guardians of both perpetrator (if known) and victim.
- Maintain dialogue with both victim and perpetrators parents.
- Accurately record and report the incident on CPOMS.
- Monitor the effectiveness of strategies to tackle incidents by analysing recurrence of incidents and specking to pupils involved in the incident for qualitative measure.
- Provide support and reassurance to the victim.
- If the perpetrator/s are known member/s of the school, we will make it clear to them that bullying behaviour will not be tolerated and deal with it in a fair and firm manner.
- If there is a group of people involved, they will be spoken to individually and as a whole group.
- It is important that pupils who have harmed another pupil, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.
- If a sanction is used, it will correlate to the seriousness of the incident and the perpetrator will be told why it is being used.
- If possible the perpetrator will be asked to remove or delete any harmful or inappropriate content immediately.
- If content has been published the service provider may be contacted to remove it.
- If the content includes child sexual abuse imagery, nudity or criminally obscene material the Internet Watch Foundation will be contacted to have this content removed https://www.iwf.org.uk/.
- If the content has included an adult acting inappropriately, particularly in a sexual way or arranging to meet a child we will contact CEOP https://ceop.police.uk.
- The perpetrator/s may have their school media access suspended.
- Repeated bullying incidents (of any form) or ones of significant severity may result in a fixed-term or permanent exclusion of the perpetrator.

7.6 Legality of Cyberbullying

Cyberbullying, whilst not being a specific criminal offence under UK law, there are a range of laws which criminalise malicious communications, stalking, threatening violence, discrimination, harassment and incitement.

Where laws have been broken, the decision will be made, usually with parents, on the need to involve Police.

7.7 How will we teach children about Bullying/Cyberbullying

There are explicit links and overlaps between teaching about Cyberbullying/ Digital Resilience within computing curriculum and personal, social and health education, citizenship, other curriculum areas, assemblies and external visitors the school.

7.8 Resources to deal with Cyberbullying

The school will use the following as resources for dealing with bullying:

- http://www.childnet.com
- http://www.childnet.com/ufiles/Cyberbullying-guidance2.pdf

Section 8
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.

8.1 Parent tips regarding Online Gaming – Taken from Britannica Learning

- Beware of gaming sites that ask you to reveal personal details of information.
- Beware of online bullies/trolls, they also operate in these environments.
- Don't forget that some of the people 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.

Section 9
Sexting

This section is written using information taken directly from the UKCCIS Sexting: Guidance for Schools and Colleges.

Newport Primary School takes the topic of 'Sexting' very seriously. Even at primary level we understand that it has become an unfortunate part of growing up in the digital age.

As described in the UKCISS Guidance, there are many different types of, and definitions for, sexting and it is likely that no two cases will be the same. It is therefore necessary to carefully consider each case on its own merit. It is important to apply a consistent approach when dealing with an incident to help protect staff, the school, and more importantly the pupil. The range of contributory factors in each case also needs to be considered in order to determine an appropriate and proportionate response. All staff should be familiar with this section of the Digital Resilience Strategy.

9.1 Sexting - Steps to take when dealing with an incident of sexting

The definition of 'sexting':

There are a number of definitions of sexting but for the purposes of this advice sexting 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

Sexting 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, followed by 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 also 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?
- Have 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 Resilience 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 freedom 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 Resilience 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 are recorded on CPOMS.
- Always put the child first. Do not search the device if this will cause additional stress to the child/pupil 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 issue.
- Print out any material for evidence.
- Save any material to a school network.
- Move any material from one storage device to another.

Staff should always:

- Inform the school’s Designated Safeguarding Lead.
- Record the incident.
- Act in accordance with school Safeguarding Policy and procedures.
- Inform relevant colleagues/senior leadership team about the alleged incident before searching a device.
- Inform the pupil’s 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 a victim of grooming with intent to meeting a pupil, then you should report this 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 Resilience 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 sexting – 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 01642 726004 if needed.
- Contact the police (if appropriate) 101.
- Put the necessary safeguards in place for the child, e.g. they may need counselling support or 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 to CEOP. www.ceop.police.uk.

Section 10

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 Sexting

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/