



## DIGITAL RESILIENCE STRATEGY - QUICK READ

### Introduction

This 'Quick Read' strategy is designed to be a simple overview to the Digital Resilience Strategy which regulates all digital activity in Newport Primary School. It is a short guide to the key information and does not replace the Digital Resilience Strategy.

### What is meant by '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 they (pupils) might be exposed to when they are using social media or going online"

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 Resilience covers use of the internet, mobile phones and other electronic communications technologies including tablets and gaming consoles.

### Computing curriculum

The whole school curriculum long-term overview document details what pupils should be learning in computing and should be referred to when planning.

The Computing Subject Leader can support with effectively planning, delivering and assessing the computing curriculum.

### 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.
- Pupils receive digital safeguarding lessons through the computing curriculum, RHE lessons, circle time and other curriculum areas and are frequently reminded of being safe online and being a good digital citizen.
- The school utilises the 'Be Internet Legends' programme to teach children to explore the online world ([Be Internet Legends - A Program to Teach Children Internet Safety](http://beinternetawesome.withgoogle.com))

## **Ensuring safe internet access**

The IT systems in Newport Primary School are managed by One IT Services.

Newport Primary School has Blocking and/or filtering software. The HT/DHT receive reports if inappropriate material has been accessed. If staff or pupils discover an unsuitable site, it must be reported to the schools DSL. This will be reported to One IT Solutions by the DSL. Any material that the school suspects is illegal will be referred to Report Remove Internet Watch Foundation [IWF - Welcome to the IWF](#)

## **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 uses Microsoft Teams for internal messaging 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.

## **Social Networking**

Social networking sites, bulletin boards, forums, video conferencing, chat rooms and instant messaging applications are all strictly prohibited on school devices or network, other than use of the school's official Facebook page.

### **Safeguarding pupils in the context of social media**

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

- Contact

- Conduct
- Content
- Commercialism

For detailed information, refer to the computing curriculum and/or speak to the Computing Subject Leader.

## **Staff Social Networking**

Newport Primary School does not wish to discourage staff from using social media sites and applications in their own personal time, we do however aim to protect staff from the pitfalls of inappropriate use, and we do expect certain standards of conduct to be observed.

Accessing social networking sites in work time, using school IT internet connections is strictly forbidden, using the schools IT equipment to access social networking either at home or at the school is also strictly prohibited, unless this is directly linked to school related activity.

The term 'staff' covers all employees of the school, including casual staff, agency employees and volunteers.

When using social media, the school prohibits staff from accepting invitations from pupils, or pupil's family members and friends. Staff must also not initiate any contact or accept online friend requests with pupils or pupil's family members or friends under any circumstances.

## **Content of interactions**

When staff are interacting with social media the following points must be adhered to:

- Staff should not make direct references on social networking sites to the school, its staff, pupils or their families. Sharing of posts from the School Facebook Page is permitted providing this is done within a positive context and does not contain any negative, derogatory or offensive comments.
- 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 interpreted as confidential to the school, staff, pupils or their families or which could be deemed or interpreted as derogatory, defamatory or discriminatory. They should not post comments or entries onto social networking sites in 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.

### **Social Networking and Preventing Radicalisation**

Our children may actively search, come across by accident or be persuaded by others to look for content that is considered radical such as Far-Right, Far-left, Islamic extremist, terrorist training materials and videos glorifying war and Incel groups. The internet/social media platforms can be used to build rapport with young people in order to radicalise them.

#### **What are the signs to look out for?**

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.

#### **Reporting**

**Online terrorism:** You can report terrorism related content to the police's Counter Terrorism Internet Referral Unit at [www.gov.uk/report-terrorism](http://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](http://www.report-it.org.uk).

## **Mobile devices: Staff, pupils and parents**

### **Staff**

- Staff must not use mobile phones in classrooms at any time when pupils are present
- Staff are permitted to use their devices in staff rooms, meeting rooms or classrooms during break and lunchtime if no pupils are present
- 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.

### **Pupils**

Pupils are not permitted to bring mobile devices into the school, unless it is with the express permission of the Headteacher or Deputy Headteacher in exceptional circumstances.

### **Parents**

The school will encourage a policy for parents to 'Greet your child with a smile not a phone' when collecting children at the end of the school day.

## **Specific Digital Safeguarding issues**

### **Child-on-child Abuse**

All staff should be aware that safeguarding issues can manifest themselves via child-on-child abuse. This is most likely to include, but may not be limited to:

- Bullying (including cyber bullying)
- Sexual harassment such as sexual comments, remarks, jokes and online sexual harassment, which may be stand-alone or part of a broader pattern of abuse
- Upskirting which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
- Sharing of nudes or semi-nudes (sexting)

Concerns relating to child-on-child abuse should be reported immediately to the DSL and recorded on CPOMS.

### **Online Child Sexual Exploitation and Child Criminal Exploitation (Online CSE and CCE)**

Online CSE is a form of sexual abuse where children are sexually exploited in exchange for money, power or status.

Child criminal exploitation (CCE) is a form of abuse where an individual or group takes advantage of an imbalance of power to coerce, control, manipulate or deceive a child into criminal activity, in

exchange for something the victim needs or wants, and/or for the financial or other advantage of the perpetrator or facilitator, and/or through violence or the threat of violence.

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.

Indicators of CCE can include a child:

- Appearing with unexplained gifts or new possessions
- Associating with other young people involved in exploitation
- Suffering from changes in emotional wellbeing
- Misusing drugs and alcohol
- Going missing for periods of time or regularly coming home late
- Regularly missing school or education
- Not taking part in education

All Incidents of online CSE and CCE should be reported to the schools Designated Safeguarding Lead (DSL).

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.

## **Cyberbullying and trolling**

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.

## **Spotting the signs of Cyberbullying**

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.

### **School strategy on dealing with Cyberbullying**

- Tell someone
- Do not reply – do not retaliate
- Block the bullies
- Keep the evidence

### **Dealing with Cyberbullying**

If an allegation of child-on-child abuse or bullying does come up, this should be reported to the DSL and be recorded on CPOMS.

- If the content includes child sexual abuse imagery, nudity or criminally obscene material the Report Remove tool from the Internet Watch Foundation will be contacted to have this content removed [IWF - Welcome to the IWF](#)
- 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>.

### **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>
- Be Internet Legends [Be Internet Legends - A Program to Teach Children Internet Safety \(beinternetawesome.withgoogle.com\)](#)

### **Sharing of nudes and semi-nudes ('Sexting')**

There are a number of definitions of sharing of nudes and semi-nudes ('sexting'): but for the purposes of this advice it 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**

Sharing of nudes and semi-nudes ('sexting'): disclosures should follow our normal safeguarding practices in lines with the schools Safeguarding and Child Protection Policy.

A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or pornography. As a general rule, staff should NEVER search a device, this should be done by a member of the safeguarding team unless there is an immediate safeguarding issue.

If content includes child sexual abuse imagery, nudity or criminally obscene material the Report Remove 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>.

### **Who should deal with the incident?**

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.

### **Use of Artificial Intelligence**

When we use AI in school we follow the 5 principles set out in the AI regulation white paper.

Regulatory principle	WE WILL ...
Safety, security and robustness	<ul style="list-style-type: none"> <li>• Ensure that AI solutions are secure and safe for users and protect users' data</li> <li>• Ensure we can identify and rectify bias or error</li> <li>• Anticipate threats such as hacking</li> </ul>
Appropriate transparency and explainability	<ul style="list-style-type: none"> <li>• Be transparent about our use of AI, and make sure we understand the suggestions it makes</li> </ul>
Fairness	<ul style="list-style-type: none"> <li>• Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate</li> </ul>
Accountability and governance	<ul style="list-style-type: none"> <li>• Ensure that the governing board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI</li> </ul>

Regulatory principle	WE WILL ...
Contestability and redress	<ul style="list-style-type: none"> <li>• Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology</li> <li>• Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment</li> </ul>

### **Staff and Governor Use of AI**

As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert.

Staff have been provided with guiding principles for the use of AI in school.

### **Pupil Use of AI**

We recognise that AI has many uses to help pupils learn.

Pupils may use AI tools:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools:

- During assessments
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)

This list of AI misuse is not exhaustive.

### **Useful Sites**

Child Sexual Exploitation

Child Exploitation and Online Protection

[www.ceop.police.uk/safety-centre](http://www.ceop.police.uk/safety-centre)

Childline

[www.childline.org.uk](http://www.childline.org.uk)

The Internet Watch Foundation

<https://www.iwf.org.uk/what-we-do/why-we-exist/report-remove>

## Specific Safeguarding Issues

Cyberbullying, Online CSE, Radicalisation, Inappropriate Content

Childnet

[www.childnet.com](http://www.childnet.com)

Think U Know – Resource Library on CSE and Cyberbullying

[www.thinkuknow.co.uk/professionals](http://www.thinkuknow.co.uk/professionals)

Guidance and Resources on Sharing Nudes and Semi-nudes ('Sexting')

[www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis](http://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis)

Childline

[www.childline.org.uk](http://www.childline.org.uk)

[Parent Zone](#)

<https://nationalonlinesafety.com/guides>