Online Safety Policy

St Vincent's Catholic Primary School

The School Mission Statement

To love, serve and learn as Jesus shows us

DOCUMENT STATUS

Drafted:	Last review:	Adopted by Governors:	Implemented:	Next review:
February 2016 (original policy) February 2021 (current policy)	February 2022	March 2021	March 2021	February 2023

Contents:

Appendices

Statement of intent

St Vincent’s understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

1.1 This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

1.2 This policy operates in conjunction with the following school policies:

- Child Protection and Safeguarding Policy
- Managing Allegations of Abuse Against Staff Policy
- Acceptable Use Policy and Agreements
- Anti-Bullying Policy
- RSHE Policy
- Staff Code of Conduct
- Home-Achool Agreement
- Behaviour Policy
- Disciplinary Policy
- Data Protection Policy
- Mobile Phone Policy
- Preventing Extremism and Radicalisation Policy
- Remote Learning Policy

2. Roles and responsibilities

2.1. The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

2.2. The Head Teacher / DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the Computing lead and IT technician.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing body about online safety on a termly basis.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are evaluated.
- Supporting staff to ensure that online safety is embedded so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the ICT technicians to review this policy.
- Working with the Governing Body to update this policy on an annual basis.

2.3. ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety procedures.
- Implementing appropriate security measures as directed by the Head Teacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the Head Teacher to review this policy

2.4. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2.5. Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online at school or at home.
- Using devices, software and apps sensibly and with the consent of an adult.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

3.1. Online safety is embedded throughout the curriculum; however, it is particularly addressed in Computing and RSHE, and through Digital Wellbeing Week, Safer Internet Day and Anti-bullying Week

3.2. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

3.3. Online safety teaching is taught to all age groups and is always appropriate to pupils' ages and developmental stages.

3.4. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

3.5. The risks pupils may face online are always considered when developing the curriculum.

3.6. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

3.7. External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum.

3.8. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering in this way. The staff member will be advised on how to best support any pupil who may be especially impacted by a lesson or activity.

3.9. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

3.10. During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

3.11. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make inform the DSL.

3.12. If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

4. Staff training

4.1. All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

4.2. Online safety training for staff is updated annually and is delivered in line with advice from the three local safeguarding partners.

4.3. In addition to this training, staff also receive regular online safety updates as required.

4.4. In addition to this formal training, the DSL receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

4.5. All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

4.6. Staff are required to adhere to the Acceptable Use Policy at all times, which includes provisions for the acceptable use of technologies and the use of social media.

4.7. All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

4.8. The DSL acts as the first point of contact for staff requiring advice about online safety.

5. Educating parents

5.1. The school works in partnership with parents to ensure pupils stay safe online at school and at home.

5.2. Parents are provided with information about the school’s approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Parents workshops
- Newsletters
- School Twitter page

6. Classroom use

6.1. A range of technology is used during lessons, including laptops and tablets

6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. .

6.3. Pupils are supervised when using online materials during lesson time.

7. Internet access

7.1. Pupils, staff and other members of the school community are granted access to the school's internet network once they have read and signed the Acceptable Use Agreement (Appendices 2 and 3).

7.2. All members of the school community are encouraged to use the school's internet network, instead of mobile phone networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

8. Filtering and monitoring online activity

8.1. St. Vincent's Catholic Primary School uses Warrington Borough Council's actively monitored and filtered internet service, which reduces the risk of pupils encountering unsuitable material in school. See information in Appendix 4.

8.2. The Governing Body ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

8.3. ICT technicians undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

8.4. Requests regarding making changes to the filtering system are directed to the Head Teacher.

8.5. Reports of inappropriate websites or materials are made to the ICT technician immediately, who investigates the matter and makes any necessary changes.

8.6. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy.

8.7. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the school's Disciplinary Procedure.

8.8. All users of the network and school-owned devices are informed about how and why they are monitored.

9. Network security

9.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.

9.2. Firewalls are switched on at all times.

9.3. ICT technicians review the firewalls to ensure they are running correctly, and to carry out any required updates.

9.4. Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.

9.5. Staff members and pupils report all malware and virus attacks to ICT technicians and the Head Teacher.

9.6. All members of staff have their own unique usernames and private passwords to access the school's systems.

9.7. Pupils are provided with their own unique username and private passwords.

9.8. Staff members and pupils are responsible for keeping their passwords private.

9.9. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

9.10. Staff are required to lock access to devices and systems when they are not in use.

10. Emails

10.1. Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

10.2. Prior to being authorised to use the email system, staff must agree to and sign the relevant acceptable use agreement.

10.3. Class teachers will teach a session explaining what a phishing email and other malicious emails might look like – includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

11. Social networking

Personal use

11.1. Access to social networking sites is filtered as appropriate.

11.2. Staff receive training on how to use social media safely and responsibly.

11.3. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

11.4. Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

11.5. Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

Use on behalf of the school

11.6. Consent from parent or carers must be obtained before photographs of pupils are published on the school twitter page. Parents can withdraw permission at any time.

11.7. The school's official social media channels are only used for official educational or engagement purposes.

11.8. Photographs that include pupils will be selected carefully.

11.9. Pupil's full names will not be used anywhere on the school Twitter page or website, particularly in association with photographs.

11.10. Staff members must be authorised by the headteacher to access to the school's social media accounts.

12. The school website

12.1. The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

12.2. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

12.3. Personal information relating to staff and pupils is not published on the website.

13. Remote Learning

13.1. Children may be required to complete learning remotely, as part of homework or during periods of school closure.

13.2. During periods of remote learning, the Remote Learning Policy will be followed

13.3. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are not permitted unless in exceptional circumstances and approved by the Head Teacher or Deputy Head Teacher. Staff will not be alone if communicating with an individual child using video communication
- Wear suitable clothing – this includes others in their household
- Be seated in a suitable location for learning – bedrooms are not an appropriate location
- Use appropriate language – this includes others in their household
- Maintain the standard of behaviour expected in school
- Use the necessary equipment and computer programs as intended e.g. the text chat facility must only be used in relation to learning, to ask questions / make statements
- Not record, store, or distribute video material or any digital content without permission
- Always remain aware that they are visible
- Be free from distraction so that they can focus on the session and activity in the background should be kept to a minimum
- Mute their microphone unless they are speaking; children must use the “hand up” tool to indicate that they wish to speak as they would in school
- Children must leave the session when it is ended
- An adult must supervise children engaged in a video communication but should not engage within the session

13.4. All staff and pupils using audio communication (online or telephone) must:

- Use appropriate language – this includes others in their household
- Maintain the standard of behaviour expected in school
- Use the necessary equipment and computer programs as intended
- Not record, store, or distribute audio material without permission
- Ensure they have a stable connection to avoid disruption to lessons
- Always remain aware that they can be heard

13.5. During the period of remote learning, the school will continue to:

- Reinforce the importance of children staying safe online
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious website

14. Use of school-owned devices

14.1. Staff members are issued with the following devices to assist with their work: Laptop and ipad

14.2. Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

14.3. All school-owned devices are password protected.

14.4. ICT technicians review school-owned devices to carry out software updates.

14.5. No software, apps or other programmes can be downloaded onto a device without authorisation from Computing Subject Lead or ICT technicians.

15. Use of personal devices

15.1. Any personal electronic device that is brought into school is the responsibility of the user.

15.2. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency.

15.3. As teachers possess their own ipad, they should not use their personal devices to take photos or videos of pupils.

15.4. Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.

15.5. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

16. Responding to specific online safety concerns

Cyberbullying

16.1. Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

16.2. Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Online sexual violence and sexual harassment between children (child-on-child abuse)

16.3 Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

16.4 The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person’s clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

16.5 Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

16.6 The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Peer-on-peer Abuse Policy and the Child Protection and Safeguarding Policy.

Online abuse and exploitation

16.7. Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

16.8. Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.

- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

16.9. Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

16.10. Child sexual exploitation (CSE) and child criminal exploitation (CCE)

- Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.
- CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
- Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

16.11. Radicalisation

- Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.
- Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.
- Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.
- Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.
- The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.
- All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Safeguarding Policy.

Online hate

16.12. The school does not tolerate online hate content directed towards or posted by members of the school community.

16.13. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved.

17. Mental health

17.1. The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

17.2. Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Mental Health and Emotional Wellbeing Policy.

18. Online hoaxes and harmful online challenges

18.1. For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

18.2. For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

18.3. Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

18.4. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

18.5. Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

18.6. Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

18.7. The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

19. Cyber-crime

19.1. Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- *Cyber-enabled* – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- *Cyber-dependent* – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

19.2. The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

19.3. The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

20. Monitoring and review

20.1. The school recognises that the online world is constantly changing; therefore, the Head Teacher / DSL, and ICT technicians conduct light-touch reviews of this policy to evaluate its effectiveness.

20.2. The Governing Body and Head Teacher will review this policy in full on an annual basis and following any online safety incidents.

20.3. Any changes made to this policy are communicated to all members of the school community.

Appendix 1: Online harms and risks – curriculum coverage

The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about.

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: ● That age verification exists and why some online platforms ask users to verify their age ● Why age restrictions exist ● That content that requires age verification can be damaging to under-age consumers ● What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum area(s): RSHE and Computing ● Health education ● Computing curriculum
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: ● What a digital footprint is, how it develops and how it can affect pupils' futures ● How cookies work ● How content can be shared, tagged and traced ● How difficult it is to remove something once it has been shared online ● What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Health education ● Computing curriculum
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: ● Disinformation and why individuals or groups choose to share false information in order to deliberately deceive ● Misinformation and being aware that false and misleading information can be shared inadvertently ● Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons ● That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online ● How to measure and check authenticity online ● The potential consequences of sharing information that may not be true	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Health education ● KS2 Computing curriculum

Fake websites and scam emails	Fake websites and scam e mails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: ● How to recognise fake URLs and websites ● What secure markings on websites are and how to assess the sources of emails ● The risks of entering information to a website which is not secure ● What pupils should do if they are harmed/targeted/groomed as a result of interacting with a fake website or scam email ● Who pupils should go to for support	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Health education ● Computing curriculum
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: ● Why passwords are important, how to keep them safe and that others might try to get people to reveal them ● How to recognise phishing scams ● The importance of online security to protect against viruses that are designed to gain access to password information ● What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Computing curriculum
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: ● How cookies work ● How data is farmed from sources which look neutral ● How and why personal data is shared by online companies ● How pupils can protect themselves and that acting quickly is essential when something happens ● The rights children have with regards to their data ● How to limit the data companies can gather	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Computing curriculum
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: ● That the majority of games and platforms are designed to make money – their primary driver is to encourage people to stay online for as long as possible ● How notifications are used to pull users back online	This risk or harm is covered in the following curriculum area(s): ● Health education ● Computing curriculum

Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: ● How to find information about privacy settings on various devices and platforms ● That privacy settings have limitations	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Computing curriculum
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: ● How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts ● How the targeting is done ● The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum area(s): ● Health education ● Computing curriculum
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: ● The types of online abuse, including sexual harassment, bullying, trolling and intimidation ● When online abuse can become illegal ● How to respond to online abuse and how to access support ● How to respond when the abuse is anonymous ● The potential implications of online abuse ● What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Health education ● Computing curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: ● What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal ● How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why ● That it is okay to say no and to not take part in a challenge ● How and where to go for help ● The importance of telling an adult about challenges which include threats or secrecy – ‘chain letter’ style challenges	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Health education
Content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: ● That online content (sometimes gang related)	This risk or harm is covered in the following curriculum area(s):

	can glamorise the possession of weapons and drugs ● That to intentionally encourage or assist in an offence is also a criminal offence ● How and where to get help if they are worried about involvement in violence	● Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: ● That, in some cases, profiles may be people posing as someone they are not or may be 'bots' ● How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Computing curriculum
Live streaming	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: ● What the risks of carrying out live streaming are, e.g. the potential for people to record livestreams and share the content ● The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely ● That online behaviours should mirror offline behaviours and that this should be considered when making a livestream ● That pupils should not feel pressured to do something online that they would not do offline ● Why people sometimes do and say things online that they would never consider appropriate offline ● The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next ● The risks of grooming	This risk or harm is covered in the following curriculum area(s): ● Relationships education
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: ● That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with ● How to identify indicators of risk and unsafe communications ● The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before	This risk or harm is covered in the following curriculum area(s): ● Relationships education ● Computing curriculum

	● What online consent is and how to develop strategies to confidently say no to both friends and strangers online	
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to ‘unrealistic’ online images. Teaching includes the following: ● The issue of using image filters and digital enhancement ● The role of social media influencers, including that they are paid to influence the behaviour of their followers ● The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum area(s): ● **Computing Curriculum**
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: ● How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) ● How to consider quality vs. quantity of online activity ● The need for pupils to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear or missing out ● That time spent online gives users less time to do other activities, which can lead some users to become physically inactive ● The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues ● That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support ● Where to get help	This risk or harm is covered in the following curriculum area(s): ● Health education
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: ● How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives ● How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum area(s): ● Relationships education

Appendix 2: Staff Acceptable Use Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology and the school systems, they are asked to read the Acceptable Use Policy and sign this agreement.

This is not an exhaustive list and all members of staff are reminded that technology use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters (both upper and lower case) and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the e-safety policy and will always take into account parental consent.
- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), in line with GDPR and the Acceptable Use Policy. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the school computer system or school-provided laptop that is unrelated to school activities, such as personal photographs, files or financial information.
- I will respect copyright and intellectual property rights.
- I have read and understood the school Online Safety Policy which covers the requirements for safe use of technology, including using appropriate devices, safe use of social media websites, such as Twitter and Facebook and the supervision of pupils within the classroom and other working spaces.
- I will report all incidents of concern regarding children's online safety to the DSL as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the DSL or EDAC Solutions (IT support) as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team (EDAC Solutions) as soon as possible.
- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Staff must not have pupils or parents as 'Friends' on Facebook. Any pre-existing relationships which may compromise this must be discussed with the Senior Leadership team.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.
- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Council, into disrepute.
- I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Head Teacher.
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

USE OF PERSONAL AND NON-SCHOOL IT EQUIPMENT

The use of non-school and personal IT equipment to undertake school business brings both opportunities and risks. The potential for an increase in flexibility and convenience must be balanced against the need to keep personal and sensitive information secure. You must only use your personal hand held/external devices (mobile phones/USB devices etc.) in school if permission has been gained from the head teacher in line with the Acceptable Use Policy. Employees must understand that, if they do use their own devices in school, they will follow the rules set out in this agreement, in the same way as if they were using school equipment in terms of monitoring and accountability; you must keep personal phone numbers and email accounts private and not use your own mobile phones or email accounts to contact pupils;

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff IT Acceptable Use Policy.

Signed: ……………………….....…… Print Name: …………………………………

Date: ………

Accepted by: ………………………………. Print Name: ……………………………..

Date: ………

Appendix 3: Pupil Acceptable Use Agreement

All pupils must follow the rules in this policy when using school laptops and iPad devices.

Pupils that do not follow these rules may find:

- They are not allowed to use the devices,
- They can only use the devices if under direct supervision. Their teachers will show pupils how to use the devices.

Devices Rules	
1	I will only use polite language when using the devices.
2	I must not write anything that might: upset someone or give the school a bad name.
3	I know that the teachers will regularly check what I have done on the school devices.
4	I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the devices before.
5	I must not tell anyone my name, where I live, or my telephone number - over the Internet.
6	I must not tell my username and passwords to anyone else but my parents.
7	I must never use other people's usernames and passwords or computers left logged in by them.
8	If I think someone has learned my password then I will tell *my teacher.*
9	I must log off after I have finished with my device.
10	I know that e-mail is not guaranteed to be private. I must not send unnamed e-mails.
11	I must not use the devices in any way that stops other people using them.
12	I will report any websites that make me feel uncomfortable to my teacher or Head Teacher
13	I will tell my teacher or Head Teacher straight away if I am sent any messages that make me feel uncomfortable.
14	I will not try to harm any equipment or the work of another person on a device.
15	If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.
16	I will not pretend to be anyone else when using devices and the internet.
17	I will not upload anything to the internet on the school devices unless instructed to do so.
18	I will not bring my own devices into school and use any mobile network connections to access the internet in school.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Waste time or resources on school computers.
- Uploading anything, including pictures of other people, to the internet, without asking my teachers first

Pupil User Acceptable Use Agreement Form

I agree to follow the school rules when using the school devices.

I will use the network in a sensible way and follow all the rules explained by my teacher.

I agree to report anyone not using the devices sensibly to my teacher.

I also agree to tell my teacher, or Head Teahcer if I see any websites that make me feel unhappy or uncomfortable.

If I do not follow the rules, I understand that this may mean I might not be able to use the devices.

Student Name: ____

Date: __/__ /

I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the devices may have their use stopped, more closely monitored or past use investigated.

Parent/Carer/Guardian Name:

Parent/Carer/Guardian Signature: _________________________

Date: __/__ /

Appendix 4: Appropriate Filtering for Education Settings

June 2016

Provider Checklist Reponses

Schools in England (and Wales) are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*"[1]. Furthermore, the Department for Education published the revised statutory guidance 'Keeping Children Safe in Education'[2] in May 2016 (and active from 5th September 2016) for schools and colleges in England. Amongst the revisions, schools are obligated to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Warrington Borough Council
Address	Quattro Towers , Buttermarket Street , Warrington
Contact details	
Filtering System	Fortiguard Web Content Filtering
Date of assessment	25/11/16

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	🟩
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	🟧

.

[1] Revised Prevent Duty Guidance: for England and Wales, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf

[2] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	WBC Explanation
● Are IWF members	🟩	Fortinet is a member of the IWF
● and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)	🟩	The IWF CAIC list is part of Fortiguard Web Filtering Service. Category – Child Abuse: websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at http://www.iwf.org.uk/
● Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'	🟩	The list is part of Fortiguard Web Filtering Service.

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	WBC Explanation
Discriminatio n	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.	🟩	**Category - Discrimination** Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group. ***Sites in this category are blocked by default for schools***
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances	🟩	**Category - Drug Abuse** Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc. ***Sites in this category are blocked by default for schools***
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance	🟩	**Category - Extremist Groups** Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs

		🟩	***Sites in this category are blocked by default for schools***
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content	🟩	**Category - Malicious Websites** Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse. **Category - Hacking** Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites. ***Sites in these categories are blocked by default for schools***
Pornography	displays sexual acts or explicit images	🟩	**Category - Pornography** Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite. **Category - Nudity and Risque** Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse ***Sites in these categories are blocked by default for schools***
Piracy and copyright theft	includes illegal provision of copyrighted material	🟩	**Category - Peer-to-Peer File Sharing** Websites that allow users to share files and data storage between each other. ***Sites in this category are blocked by default for schools***
Self Harm	promotes or displays deliberate self harm (including suicide and	🟩	**Category - Explicit Violence** This category includes sites that depict

	eating disorders)	🟩	offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc ***Sites in this category are blocked by default for schools***
Violence	Displays or promotes the use of physical force intended to hurt or kill	🟩	**Category - Explicit Violence** This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc. ***Sites in this category are blocked by default for schools***

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

The following web link contains descriptions of Fortinet's normal categories:
http://www.fortiguard.com/webfilter

FortiGuard URL Database Categories are based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families. They also take into account customer requirements for Internet management. The categories are defined to be easily manageable and patterned to industry standards.

Each category contains websites or web pages that have been assigned based on their dominant Web content. A website or webpage is categorized into a specific category that is likely to be blocked according to its content. When a website contains elements in different categories, web pages on the site are separately categorized.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

The policies which we use for schools have been carefully tailored to enable access to the majority of appropriate websites. On the occasion where a school is unable to access a specific website, the school is able to either unblock the website themselves if they have requested this level of access or contact our service desk to request the site be unblocked.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	WBC Explanation
● Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role	🟩	Policies can be adjusted to account for different, requirements, use groups, times of day etc.

- Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content	🟩	All schools have the option of managing their own Block and Permit policies.
- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking	🟩	The general categories are published on Fortinet's web site: http://www.fortiguard.com/webfilter
- Identification - the filtering system should have the ability to identify users	🟩	Users are identified via IP address.
- Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies	🟩	The Fortinet service is in-line with our internet feed so all internet data both egress and ingress passes through the filter.
- Multiple language support – the ability for the system to manage relevant languages	🟩	The Fortinet web filtering system has multi-language allowing effective filtering to occur regardless of the language the user is using or the page being visited.
- Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices	🟩	No clients or agents are required on any endpoint to ensure the filtering is enforced
- Reporting mechanism – the ability to report inappropriate content for access or blocking	🟩	We implement a standard block page, and schools can either unblock or report the issue to us via our service desk for the site to be unblocked Where inappropriate access has occurred, again the school can block this site if they have requested that level of access, or contact our service desk for the site to be blocked.
- Reports – the system offers clear historical information on the websites visited by your users	🟩	The system offers a broad range of reports which schools can request. Historical data is stored for a set period of time and reports ran against this data.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum".*[3]

Please note below opportunities to support schools (and other settings) in this regard

Support can be accessed from Warrington Borough Council's ICT Team or the Education Safeguarding Team.

[3] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements, the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a person or persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the service or its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elements of a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	David Gallear
Position	Networks Technical Lead
Date	25/11/2016
Signature	