

# Online Safety Policy



## St Vincent's Catholic Primary School

### The School Mission Statement

*To love, serve and learn as Jesus shows us*

### DOCUMENT STATUS

<u>Adopted and implemented by Governors:</u>	<u>Last reviewed:</u>	<u>Next review:</u>
February 2016	February 2023	February 2024

# Contents:

## Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Child-on-child sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. [Online safety and the curriculum](#)
12. [Use of technology in the classroom](#)
13. [Use of smart technology](#)
14. [Educating parents](#)
15. [Internet access](#)
16. [Filtering and monitoring online activity](#)
17. [Network security](#)
18. [Emails](#)
19. [Social networking](#)
20. [The school website](#)
21. [Use of devices](#)
22. [Remote learning](#)
23. [Monitoring and review](#)

## **Appendix**

- A. [Online harms and risks – curriculum coverage](#)
- B. Staff Acceptable Use Agreement
- C. Pupil Acceptable Use Agreement
- D. Appropriate Filtering for Educational Settings – Provider Response

## Statement of intent

St Vincent's Catholic Primary School 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 four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **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

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 (2022) 'Keeping children safe in education 2022'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- 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'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Acceptable Use Policy and Agreements
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Home-School Agreement
- Behaviour Policy
- Disciplinary Policy and Procedures
- Mobile Phone Policy
- Social Media Policy
- RSHE Policy
- Mental Health and Emotional Wellbeing Policy
- Data Protection Policy
- Preventing Extremism and Radicalisation Policy
- Remote Learning Policy

# 2. Roles and responsibilities

The governing board will be 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 and at regular intervals.
- 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.

The headteacher will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- 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 audited and evaluated.
- 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 DSL and IT technician to conduct light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

- Taking the lead responsibility for online safety in the school.
- 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 SENCO and IT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this 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 board about online safety on a termly basis.
- Working with the headteacher and IT technician to conduct light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.

IT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and headteacher to conduct light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of IT 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, the 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.

Pupils will be 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 have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

### **3. Managing online safety**

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies / focus days on the topic of remaining safe online

#### **Handling online safety concerns**

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and IT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

## **4. Cyberbullying**

Cyberbullying can include, but is not limited to, 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
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

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.

## **5. Child-on-child sexual abuse and harassment**

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, 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.

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
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

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.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

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

## **6. Grooming and exploitation**

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.

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, e.g. 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.

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 online.
- 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.

### **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.

### **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 Preventing Extremism and Radicalisation 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 Preventing Extremism and Radicalisation Policy.

## 7. Mental health

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.

## 8. Online hoaxes and harmful online challenges

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.

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.

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.

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.

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.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, 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 individual pupils at risk where appropriate.

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.

## 9. Cyber-crime

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.

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.

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

## 10. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

## 11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in Computing and RSHE and through theme weeks and focus days.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

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. 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
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in [appendix A](#) of this policy.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

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

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

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

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

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

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 the Child Protection and Safeguarding Policy.

## **12. Use of technology in the classroom**

A wide range of technology will be used during lessons, including the following:

- Laptops
- Tablets
- Internet
- Email
- Cameras

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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

### **13. Use of smart technology**

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of devices.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom or on school site.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

### **14. Educating parents**

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Information sessions
- Newsletters
- Online resources

### **15. Internet access**

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement or school has signed parental consent. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

## **16. Filtering and monitoring online activity**

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.

The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

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

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, IT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by IT technicians. Reports of inappropriate websites or materials will be made to an IT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and IT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

## **17. Network security**

Technical security features, such as anti-virus software, will be kept up-to-date and managed by IT technicians. Firewalls will be switched on at all times. IT technicians will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to IT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in Key Stage 2 will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after 90 days, after which users will be required to change them.

Users will inform IT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

## **18. Emails**

Access to and the use of emails will be managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to IT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Theme days and weeks, and computing teaching will remind children about what phishing emails and other malicious emails might look like including:

- 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

## **19. Social networking**

The use of social media by staff and pupils will be managed in line with the school's Social Media Policy.

## **20. The school website**

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

## **21. Use of devices**

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Acceptable Use Agreement.

## **22. Remote learning**

All remote learning will be delivered in line with the school's Remote Learning Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

## **23. Monitoring and review**

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

The governing board, headteacher and DSL will review this policy in full on an annual basis and following any online safety incidents.

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

# 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
<b>How to navigate the internet and manage information</b>		
Age restrictions	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That age verification exists and why some online platforms ask users to verify their age</li> <li>• Why age restrictions exist</li> <li>• That content that requires age verification can be damaging to under-age consumers</li> <li>• What the age of digital consent is (13 for most platforms) and why it is important</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• What a digital footprint is, how it develops and how it can affect pupils' futures</li> <li>• How cookies work</li> <li>• How content can be shared, tagged and traced</li> <li>• How difficult it is to remove something once it has been shared online</li> <li>• What is illegal online, e.g. youth-produced sexual imagery (sexting)</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive</li> <li>• Misinformation and being aware that false and misleading information can be shared inadvertently</li> <li>• Malinformation and understanding that some genuine information can be published with the deliberate intent to harm, e.g. releasing private information or photographs</li> <li>• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons</li> <li>• 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</li> <li>• How to measure and check authenticity online</li> <li>• The potential consequences of sharing information that may not be true</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing (KS2)</li> </ul>
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by	This risk or harm will be covered in the

	<p>the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How to recognise fake URLs and websites</li> <li>• What secure markings on websites are and how to assess the sources of emails</li> <li>• The risks of entering information to a website which is not secure</li> <li>• What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email</li> <li>• Who pupils should go to for support</li> <li>• The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist</li> </ul>	<p>following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Online fraud	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• What identity fraud, scams and phishing are</li> <li>• That online fraud can be highly sophisticated and that anyone can be a victim</li> <li>• How to protect yourself and others against different types of online fraud</li> <li>• How to identify 'money mule' schemes and recruiters</li> <li>• The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal</li> <li>• The risk of sharing personal information that could be used by fraudsters</li> <li>• That children are sometimes targeted to access adults' data</li> <li>• What 'good' companies will and will not do when it comes to personal details</li> <li>• How to report fraud, phishing attempts, suspicious websites and adverts</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Password phishing	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• Why passwords are important, how to keep them safe and that others might try to get people to reveal them</li> <li>• How to recognise phishing scams</li> <li>• The importance of online security to protect against viruses that are designed to gain access to password information</li> <li>• What to do when a password is compromised or thought to be compromised</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Personal data	<p>Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How cookies work</li> <li>• How data is farmed from sources which look neutral</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>



	<ul style="list-style-type: none"> <li>• How and why personal data is shared by online companies</li> <li>• How pupils can protect themselves and that acting quickly is essential when something happens</li> <li>• The rights children have with regards to their data</li> <li>• How to limit the data companies can gather</li> </ul>	<ul style="list-style-type: none"> <li>• Computing</li> </ul>
Persuasive design	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue</li> <li>• How notifications are used to pull users back online</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Privacy settings	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How to find information about privacy settings on various sites, apps, devices and platforms</li> <li>• That privacy settings have limitations</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Targeting of online content	<p>Much of the information seen online is a result of some form of targeting. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• How the targeting is done</li> <li>• The concept of clickbait and how companies can use it to draw people to their sites and services</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
<b>How to stay safe online</b>		
Online abuse	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• The types of online abuse, including sexual harassment, bullying, trolling and intimidation</li> <li>• When online abuse can become illegal</li> <li>• How to respond to online abuse and how to access support</li> <li>• How to respond when the abuse is anonymous</li> <li>• The potential implications of online abuse</li> <li>• What acceptable and unacceptable online behaviours look like</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Radicalisation	<p>Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How to recognise extremist behaviour and content online</li> </ul>	<p>All areas of the curriculum</p>

	<ul style="list-style-type: none"> <li>• Which actions could be identified as criminal activity</li> <li>• Techniques used for persuasion</li> <li>• How to access support from trusted individuals and organisations</li> </ul>	
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal</li> <li>• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why</li> <li>• That it is okay to say no and to not take part in a challenge</li> <li>• How and where to go for help</li> <li>• The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>
Content which incites violence	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That online content (sometimes gang related) can glamorise the possession of weapons and drugs</li> <li>• That to intentionally encourage or assist in an offence is also a criminal offence</li> <li>• How and where to get help if they are worried about involvement in violence</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>
Fake profiles	<p>Not everyone online is who they say they are. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• That, in some cases, profiles may be people posing as someone they are not or may be 'bots'</li> <li>• How to look out for fake profiles</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• Boundaries in friendships with peers, in families, and with others</li> <li>• Key indicators of grooming behaviour</li> <li>• The importance of disengaging from contact with suspected grooming and telling a trusted adult</li> <li>• How and where to report grooming both in school and to the police</li> </ul> <p>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.</p>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following:</p>	<p>This risk or harm will be covered in the</p>

	<ul style="list-style-type: none"> <li>• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with</li> <li>• How to identify indicators of risk and unsafe communications</li> <li>• 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</li> <li>• What online consent is and how to develop strategies to confidently say no to both friends and strangers online</li> </ul>	<p>following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> <li>• Computing</li> </ul>
<b>Wellbeing</b>		
Impact on quality of life, physical and mental health and relationships	<p>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.</p> <p>Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)</li> <li>• How to consider quality vs. quantity of online activity</li> <li>• 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 due to the fear of missing out</li> <li>• That time spent online gives users less time to do other activities, which can lead some users to become physically inactive</li> <li>• The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues</li> <li>• 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</li> <li>• Where to get help</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face. Teaching will include the following:</p> <ul style="list-style-type: none"> <li>• How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure</li> <li>• How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face</li> </ul>	<p>This risk or harm will be covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• RSHE</li> </ul>
Suicide, self-harm and eating disorders	<p>Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.</p>	



*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 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 <i>my teacher</i> .
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 Teacher 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 Responses

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”<sup>1</sup>. Furthermore, the Department for Education published the revised statutory guidance ‘Keeping Children Safe in Education’<sup>2</sup> in May 2016 (and active from 5<sup>th</sup> 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](mailto: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.	

<sup>1</sup> 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](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance_England_Wales_V2-Interactive.pdf)

<sup>2</sup> <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
<ul style="list-style-type: none"> <li>Are IWF members</li> </ul>		Fortinet is a member of the IWF
<ul style="list-style-type: none"> <li>and block access to illegal Child Abuse Images (by actively implementing the IWF CAIC list)</li> </ul>		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 <a href="http://www.iwf.org.uk/">http://www.iwf.org.uk/</a>
<ul style="list-style-type: none"> <li>Integrate the ‘the police assessed list of unlawful terrorist content, produced on behalf of the Home Office’</li> </ul>		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
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		<b>Category - Discrimination</b>  Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.  <i><b>Sites in this category are blocked by default for schools</b></i>
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		<b>Category - Drug Abuse</b> Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc. <i><b>Sites in this category are blocked by default for schools</b></i>
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		<b>Category - Extremist Groups</b>  Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs  <i><b>Sites in this category are blocked by default for schools</b></i>

Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		<p><b>Category - Malicious Websites</b></p> <p>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.</p> <p><b>Category - Hacking</b></p> <p>Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites.</p> <p><b><i>Sites in these categories are blocked by default for schools</i></b></p>
Pornography	displays sexual acts or explicit images		<p><b>Category - Pornography</b></p> <p>Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.</p> <p><b>Category - Nudity and Risque</b></p> <p>Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse</p> <p><b><i>Sites in these categories are blocked by default for schools</i></b></p>
Piracy and copyright theft	includes illegal provision of copyrighted material		<p><b>Category - Peer-to-Peer File Sharing</b></p> <p>Websites that allow users to share files and data storage between each other.</p> <p><b><i>Sites in this category are blocked by default for schools</i></b></p>
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		<p><b>Category - Explicit Violence</b></p> <p>This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc</p> <p><b><i>Sites in this category are blocked by default for schools</i></b></p>

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

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
<ul style="list-style-type: none"> <li>Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role</li> </ul>		Policies can be adjusted to account for different, requirements, use groups, times of day etc.
<ul style="list-style-type: none"> <li>Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content</li> </ul>		All schools have the option of managing their own Block and Permit policies.
<ul style="list-style-type: none"> <li>Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking</li> </ul>		The general categories are published on Fortinet's web site: <a href="http://www.fortiguard.com/webfilter">http://www.fortiguard.com/webfilter</a>

<ul style="list-style-type: none"> <li>• Identification - the filtering system should have the ability to identify users</li> </ul>		Users are identified via IP address.
<ul style="list-style-type: none"> <li>• Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies</li> </ul>		The Fortinet service is in-line with our internet feed so all internet data both egress and ingress passes through the filter.
<ul style="list-style-type: none"> <li>• Multiple language support – the ability for the system to manage relevant languages</li> </ul>		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.
<ul style="list-style-type: none"> <li>• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices</li> </ul>		No clients or agents are required on any endpoint to ensure the filtering is enforced
<ul style="list-style-type: none"> <li>• Reporting mechanism – the ability to report inappropriate content for access or blocking</li> </ul>		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.
<ul style="list-style-type: none"> <li>• Reports – the system offers clear historical information on the websites visited by your users</li> </ul>		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”***.<sup>3</sup>

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.

<sup>3</sup> <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	