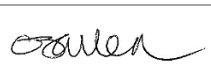
The Westbrook Trust
Achieve Together

Online Safety Policy

Version No:	2.1
Last Reviewed:	2021/22
Review Term:	1
Frequency (in years):	2
Approval Level:	Trustees
Next Review Due:	2022/23

Signed: *(Chair of Trustees)*		**Signed:** *(CEO)*	
Name:	Richard Gibbons	**Name:**	Oliver Allen
Date:	14th October 2021	**Date:**	14th October 2021

Contents

Appendices

Statement of Intent

The Westbrook Trust understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the Trust recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The use of online services is embedded throughout the Trust; therefore, there are a number of controls in place to ensure the online 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, 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. The Westbrook Trust 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 (2022) 'Keeping children safe in education 2022'
- 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, but not limited to the following school policies:

- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Safeguarding Policy
- Anti-Bullying Policy
- Child-on-Child Abuse Policy
- Low-Level Concerns Policy
- PSHE Policy
- RSE Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy
- Data Protection (GDPR) Policy
- Remote Education Policy

2. Roles & Responsibilities

2.1. The **Trustee Board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Reviewing this policy on an annual basis.
- Ensuring that the risk of online challenges and hoaxes is mitigated thorugh effective planning and incident response
- Ensuring their own knowledge of online safety issues is up-to-date.

2.2. The **Governing Board** is responsible for:

- Ensuring the DSL's remit covers online safety.
- 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.

2.3. The **Head Teacher** is 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.
- Ensuring that all staff 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.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Establishing a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.
- Engaging with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Work with the data protection officer to relation to data protection requirements.
- Working with other stakeholders e.g. ICT technicians to conduct reviews of this policy.

2.4. The **DSL** is responsible for:

- Taking the lead responsibility for online safety in the school.
- 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.

2.5. The **Deputy DSL / Online Safety Officer** is responsible for:

- 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 Head Teacher, the DSL, SENCO and ICT technicians.
- Keeping 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.
- 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.
- Working with the headteacher and ICT technicians to conduct reviews of this policy.
- Reporting to the governing board about online safety

2.6. **ICT Technicians** are 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 and On-line Safety Officer.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the Deputy DSL / Online Safety Officer and headteacher to conduct reviews of this policy.

2.7. 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, 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.
- Understanding and adhering to the Acceptable Use Agreement and Code of Conduct.

2.8. **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 have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Managing Online Safety

3.1. 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.

3.2. The DSL has overall responsibility for the school's approach to online safety, with support from the on-line safety officer 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.

3.3. 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 are conducted regularly on the topic of remaining safe online

Handling online Safety Concerns

3.4. 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 Safeguarding Policy.

3.5. Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

3.6. 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.

3.7. 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.

3.8. 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 and appropriate support provided to the victim.

3.9. 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, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, Low-Level concerns Policy and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors. If the concern is about the CEO, it is reported to the chair of Trustees.

3.10. Concerns regarding a pupil's online behaviour are reported to the on-line safety officer, who investigates concerns with relevant staff members, e.g. the DSL / headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding Policy.

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

3.12. 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 Safeguarding Policy.

4. Cyberbullying

4.1. 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
- 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
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

4.2. 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.

4.3. 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

5.1. 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.

5.2. 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

5.3. 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.

5.4. 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.

5.5. Staff 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.

5.6. The school responds 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 are 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

6.1. 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.

6.2. 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.

6.3. 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.

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

6.4. 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.

6.5. 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.

6.6. 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 Safeguarding Policy.

Radicalisation

6.7. 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.

6.8. Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Safeguarding Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

6.9. 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 Safeguarding Policy.

7. Mental Health

7.1. 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.

7.2. 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 Safeguarding Policy.

8. Online Hoaxes and Harmful Online Challenges

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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 and other colleagues about whether quick local action can prevent the hoax or challenge from spreading more widely.

8.5. 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.

8.6. 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.

8.7. 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.

9. Cyber-Crime

9.1. 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.

9.2. 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.

9.3. 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.

10. Online Safety Education

10.1. **Educating Pupils:**

- An online safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of school.
- Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.
- Pupils will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be shared prior to use.
- Pupils are instructed to report any suspicious use of the internet and digital devices to their classroom teacher.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- Schools will hold online safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

10.2. **Educating 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.
- A planned calendar programme of online safety training opportunities is available to all staff members, including whole school activities and CPD training courses. This is delivered in line with advice from the three local safeguarding partners.
- All staff will undergo regular online safety training and updates to ensure they are aware of current online safety issues and any changes to the provision of online safety, as well as current developments in social media, online gaming and the internet as a whole.
- The Deputy DSL / Online Safety Officer will regularly audit staff in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this Online Safety Policy.

- Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media and online gaming.
- All staff are informed about how to report online safety concerns, in line with the Safeguarding Policy.
- The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.
- In addition to this formal training, the DSL and any deputies 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 and their deputies 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.

10.3. **Educating Parents:**

- Schools work in partnership with parents to ensure pupils stay safe online at school and at home.
- Online safety information will be directly delivered to parents through a variety of formats, including newsletters, school websites and social media.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any online safety related concerns.
- All pupils are required to sign a copy of the Acceptable Use Agreement when they start at any of our schools. Parents are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

11. Classroom Use

11.1. A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

11.2. 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.

11.3. Class teachers ensure that any internet-derived materials are used in line with copyright law.

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

12. The Curriculum

12.1. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE
- RSE
- Computing

12.2. The curriculum and our approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

12.3. 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.

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

12.5. 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

12.6. Our Designated Safeguarding Leads (DSL's) are involved with the development of our online safety curriculum.

12.7. We recognise that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

12.8. Schools 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.

12.9. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

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

12.11. 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.

12.12. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will follow the safeguarding policy.

12.13. 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 safeguarding policy.

13. Internet Access

13.1. Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

13.2. A record is kept of users who have been granted internet access.

13.3. School owned devices should be connected to the school's internet network, and not local 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

13.4. Pupils are provided with a user account.

13.5. Pupils' activity is continuously monitored by the class teacher.

13.6. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

13.7. The use of appropriate filters and monitoring systems does not lead to 'over blocking' – unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

13.8. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the online safety co-ordinator

13.9. All school systems will be protected by up-to-date virus software.

13.10. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

14. Filtering & Monitoring Online Activity

14.1. Our IT Service Provider undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

14.2. Reports of inappropriate websites or materials are made to the online safety co-ordinator immediately, who investigate the matter and make any necessary changes.

14.3. 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.

14.4. School networks and school-owned devices are appropriately monitored.

14.5. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the relevant policy.

15. Network Security

15.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by the IT Service Provider.

15.2. Firewalls are switched on at all times. The IT Service Provider review the firewalls regularly to ensure they are running correctly, and to carry out any required updates.

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

15.4. Staff members and pupils report all malware and virus attacks to the IT Service Provider.

15.5. All members of staff have their own unique usernames and private passwords to access systems.

15.6. Staff members are responsible for keeping their passwords private.

15.7. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.

15.8. Staff passwords expire after 90 days, after which users are required to change them.

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

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

15.11. Users inform the IT Service Provider if they forget their login details, who will arrange for their password to be reset.

15.12. If a user is found to be sharing their login details or otherwise mistreating the password system, the head teacher is informed and decides the necessary action to take.

16. Emails

16.1. Access to and the use of emails is managed in line with the GDPR Policy and Acceptable Use Agreement.

16.2. Staff are given approved school email accounts and will only use these accounts for school related work.

16.3. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement.

16.4. Personal email accounts are not permitted to be used for school related work.

16.5. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

16.6. Staff members are required to report scams and suspicious emails to the IT Service Provider.

16.7. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.

16.8. Staff are advised to delete without opening all chain letters, spam and all other emails from unknown sources.

16.9. The school will provide regular education to staff and pupils regarding what a phishing email might look like – this will include information on the following:

- Determining whether or not an email address is legitimate
- Knowing the types of address a phishing email could use
- Asking "*does it urge the recipient to act immediately?*"
- Checking the spelling and grammar

16.10. In the event of a cyber-attack, the school and the IT Service Provider will investigate; however, this will be to identify the cause of the attack, any compromised data, and if there are any steps that can be taken in the future to prevent similar attacks happening.

17. Social Networking

17.1. **Personal Use:**

- Staff are encouraged to have the most private possible settings on their social media accounts.
- Access to social networking sites is filtered as appropriate.
- Staff are not permitted to use social media or online gaming sites for personal use during lesson time/working hours.
- Staff can use personal social media and online gaming sites during break and lunchtimes; however, inappropriate or excessive use may result in disciplinary action.
- Staff members are advised that their conduct on social media can have an impact on their role and reputation within school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the Trust as a whole.
- 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 or online gaming sites.
- Pupils are taught how to use social media safely and responsibly through the online safety curriculum.
- Concerns regarding the online conduct of any member of the Trust community on social media are reported to the DSL and managed in accordance with the relevant policy.

17.2. **Use on Behalf of the School:**

- Should access be needed to social networking sites during lesson time for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the head teacher.
- The school's official social media channels are only used for official educational or engagement purposes.
- Staff members must be authorised by the head teacher to access the school's social media accounts.
- All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.
- The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

18. School Websites

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

18.2. Websites comply with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies, and copyright law.

18.3. Contact details on school websites will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

18.4. Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully and will not be posted unless parents / carers have given prior authorisation.

18.5. Pupils are not permitted to take or publish photos of others without permission from the individual.

18.6. Staff are able to take pictures using school equipment. Staff will not take pictures using their personal equipment.

19. Use of School-Owned Devices

19.1. Some staff members are issued with the following devices to assist with their work:

- Laptop
- Phone
- Mobile Device

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

19.3. School-owned devices are used in accordance with the Acceptable Use Agreement.

19.4. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

19.5. All school-owned devices are password protected.

19.6. The IT Service Provider reviews all school-owned devices regularly to carry out software updates.

19.7. Software, apps or other programmes should not be downloaded onto a device without authorisation.

19.8. If staff members or pupils are found to be misusing school-owned devices, the head teacher will be informed and the appropriate policy followed.

20. Use of Personal Devices

20.1. Personal devices are used in accordance with the Staff Code of Conduct.

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

20.3. Pupils are not permitted to use personal devices throughout the school day. They are encouraged not to bring devices into school. Where this is requested by parents or carers so that pupils can be contacted on the journey to and from school, the device will be secured in the school office through the school day.

20.4. Staff members are not permitted to use their personal devices during lesson time, other than in an emergency or with prior consent by the head teacher, e.g. a school trip.

20.5. Staff members are never permitted to use their personal devices to take photos or videos of pupils.

20.6. Staff members will report concerns about their colleagues' use of personal devices on school premises in line with the Allegations of Abuse Against Staff Policy and Reporting Low Level Concerns Policy.

20.7. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the head teacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

20.8. Visitors to schools are informed of the expected use of personal devices.

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

21. Reporting Misuse

21.1. The Acceptable Use Agreement clearly defines what is classed as inappropriate behaviour. All pupils and staff members are aware of what behaviour is expected of them.

21.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to online safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

21.3. **Misuse by Pupils:**

- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the online safety coordinator using a complaints form.
- The behaviour policy will be applied and a likely suspension of internet use for any pupil who does not adhere to the rules outlined in the Acceptable Use Agreement.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding Policy.

21.4. **Misuse by Staff:**

- Any misuse of the internet by a member of staff should be immediately reported to the head teacher.
- The head teacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy and may decide to take disciplinary action against the member of staff.
- The head teacher will decide whether it is appropriate to contact any outside agencies.

21.5. **Use of Illegal Material:**

- In the event that illegal material is found on school networks, or evidence suggests that illegal material has been accessed, the police will be contacted.
- If a child protection incident is suspected, the child protection procedure will be followed – the DSL will be informed and the police contacted.

22. Remote Learning

22.1. All remote learning is delivered in line with the school's Remote Education Policy.

22.2. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with

parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

22.3. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed.

22.4. During the period of remote learning, the school will maintain regular contact with parents 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 websites.
- Direct parents to useful resources to help them keep their children safe online.

22.5. The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

An initial impact assessment under the Trust's Single Equality Scheme has been carried out for this policy	
A	Positive impact is explicitly intended and very likely
B	An adverse impact is unlikely, and on the contrary the policy has the clear potential to have a positive impact by reducing and removing barriers and inequalities that currently exist
C	An adverse impact is unlikely. On the contrary there is potential to reduce barriers and inequalities that currently exist. There is insufficient evidence, however, for this assessment to be made with as much confidence as is desirable
D	Adverse impact is unlikely, but positive impact is also unlikely.
E	Adverse impact is probable or certain, since certain groups will be disadvantaged, either proportionately or absolutely, or both. Remedial action is therefore necessary
F	Adverse impact is probable or certain for certain groups but the policy as a whole can nevertheless be justified. PLEASE NOTE: Selecting this assessment will necessitate the need for legal advice

Acceptable Use Agreement - Pupils

I will:

- Treat school equipment with care
- Follow instructions about safe use of the equipment, the internet, email, social media and online gaming sites at all times
- Only use the computers and other technology for the things that have been agreed for the lesson
- Take care not to search for anything that might be unsuitable for school or for my age
- Listen carefully and work hard when learning how to use the internet safely
- Tell if I find anything, even accidentally, that I do not think is suitable for school or for my age
- Cooperate with my parents, teachers and friends to protect members of our school community from unsafe use of the internet (including social media and online gaming)
- Never use the internet, email, online gaming sites or social media to be unkind to or bully others
- Only use the user name and password that has been issued to me
- When using email or social media, write carefully and politely
- Appreciate that everything I do on the internet or email at school can be checked by the school and that I may receive a sanction or my parent's / carers might be told if I break the rules
- Appreciate that I must take as much care at home as I do at school when using the internet (including social media and online gaming), and that if I break the rules at home, I might still receive a sanction at school

Pupil Name:	
Signature:	
Date:	

Acceptable Use Agreement – Staff

I agree to abide by the following at all times and will therefore:

- Read and adhere to The Westbrook Trust's Online Safety Policy, questioning any parts that need clarification
- Read and adhere to The Westbrook Trust's Code of Conduct
- Use computers and other technology solely for the support of educational services and not for commercial, personal or any other purposes
- Never post illegal material on the school website, whether contrary to statue or common law and never post any material which gives rise to potential liability, is contrary to school policy, or which may be inappropriate for pupils and their families
- When working with pupils, supervise them, taking all reasonable precautions to ensure that they access only appropriate material (although it is understood that it is not possible to guarantee that unsuitable material will never appear on a terminal) balancing the vast educational benefits with appropriate safeguards as set out in The Westbrook Trust's Online Safety Policy
- When working with pupils, always strive to further develop their information literacy skills so that they can recognise the bias inherent in sites and be clear about the reason for its use
- Evaluate internet content to improve future use
- Work in partnership with colleagues, parents/carers, and others to ensure that all systems to protect pupils are reviewed and improved for both home and school use
- Ensure that any misuse, including bullying, radicalisation, libel or misuse of passwords is reported and appropriate sanctions are applied
- Report unsuitable sites to the Online Safety Coordinator
- Cooperate when my use of the Internet is supervised and monitored
- Use only the email address and password that has been issued to me
- Appreciate that all incoming and outgoing emails, including my own, are public property and should not be used for personal reasons
- Always have a clear purpose for using email
- When supervising pupils, ensure that they follow email guidelines set by school
- Attend any training as required
- Adhere to the principles of the GDPR when taking work home

Staff Name:	
Signature:	
Date:	