Online Safety Policy

NEW POLICY

Date: June 2022
Review June 2023

1) Scope

At Westhoughton High School we **LEARN**:

Look after each other
Enjoy our school
Aim high
Respect each other
Never stop learning

Increasingly accessing a broad and balanced experience of education involves interaction in the online world. We want to ensure that all members of our school community are able to LEARN by using online resources safely and effectively whilst working from the school side and elsewhere.

2) Definition of online safety

Online safety is an important aspect of many different areas within school and consequently all staff and students have a responsibility to engage in a safe and responsible way. This policy follows the statutory requirements outline in KCSiE (2021) and Working together to safeguard children (2018) and non-statutory guidance, Teaching online safety in schools (2019). Effective, timely and robust online safety is fundamental to protecting children and young people in education and it is a significant part of our safeguarding agenda at Westhoughton High School.

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and schools must work hard to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting children and young people from all forms of online abuse.

Defining online abuse: "*Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones*" (NSPCC, 2019).

Hidden harms – types of online abuse may include:

- Cyberbullying
- Emotional abuse
- Grooming
- Sexting
- Sexual abuse
- Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for children in the Children Act 1989 / 2004. These are:

- Neglect
- Sexual
- Physical
- Emotional

Technology can facilitate a world of learning and development in addition to help yield a range of opportunities. However, it can also present a window to potential and actual harm and abuse and support a range of illegal abusive behaviours including, but not limited to:

- harassment
- stalking
- threatening behaviour
- creating or sharing child sexual abuse material
- inciting a child to sexual activity
- sexual exploitation
- grooming
- sexual communication with a child
- causing a child to view images or watch videos of a sexual act.

This policy should be read alongside the Westhoughton High School Safeguarding and Child Protection Policy, Acceptable Use for Students Policy and Anti-Bullying Policy.

3) Categories of online risk

Types of online risk usually fall under one of three categories:

Contact: Contact from someone online who may wish to bully or abuse the child. This could also include online grooming, online harassment or activities of a commercial nature, including tracking and harvesting person information.

Content: Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials, and misleading information or advice.

Conduct: The child may be the perpetrator of activities including: illegal downloading, hacking, gambling, financial scams, bullying or harassing another child. They might create and upload inappropriate material or provide misleading information or advice.

4)Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

The Governing Body of Westhoughton High School will:

- Support the school in ensuring that online safety remains a high priority.
- Review the online safety policy annually and ensure that the required resources are available to fully implement the policy.
- Ensure that the school has robust systems in place to monitor online safety and the safe access of staff and students to online resources and forms of communication.
- Ensure that the school is responsive to changing risks and external priorities in relation to online safety.

Headteacher/Senior Leadership Team will:

- Ensure the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated specifically to the Online Safety Lead and DSL.
- Be aware of the procedures to be followed in the event of any online safety allegation being made against a member of staff.
- Ensure that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues and students.

Online Safety Lead will:

- Oversee the co-ordination of the Westhoughton High School online safety group.
- Take responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies / documents
- Provide training and advice for staff (through both CPD and provision of support materials)
- Liaise with school technical staff to ensure appropriate safety measures/filters are in operation and that systems are regularly adapted to meet need.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments; these will be generated by the ICT support team and Pastoral support team.
- Regularly update the Safeguarding Committee with current issues, review incident logs and filtering.
- Report regularly to Senior Leadership Team
- Regularly receive updates from external agencies via online safety bulletins
- Lead pupil ambassadors in supporting our delivery of online safety
- Ensure parents are kept updated of any new technology/concerns the school becomes aware of (e.g. by the media and/or pupils/parents/carers)
- Ensure that the school is fully involved with Safer Internet Day each year

- Work alongside senior pastoral staff and DSLs to investigate and discipline regarding incidents of online abuse.

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any LA Online Safety Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis.
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the appropriate staff for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they report any suspected misuse or problem to appropriate staff for investigation.
- Safeguarding concerns are passed to a member of the safeguarding team promptly.
- all digital communications with students/ parents / carers should be on a professional level and only carried out using official school systems
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices

Designated Safeguarding Lead:

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- any other online issues that may have a safeguarding implication

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body via the CSI committee.
Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring all of the above plus ongoing improvements through use of an appropriate self-review tool

Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- respect the feelings and welfare of others, both off and online.
- take responsibility for keeping themselves and others safe online.
- are trained in using online media as a power for good, to enhance digital wellbeing
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and also to follow guidelines on the need to:

- Be responsible and accountable when taking photos/using technology at school events.
- Know who the school DSL is.
- Know how to report online issues.
- Report any incidents or issues they become aware of.
- Be a role model for safe and appropriate behaviour.
- Identify and act upon any changes in children's behaviour that could indicate they are at risk of online harm or abuse.

5) Online Safety in the Curriculum

The education of students in online safety is an essential part of the school's online safety provision. Young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
The online safety curriculum is provided in the following ways:

- Internet safety is delivered in KS3 computing programmes of study
- Online safety, Positive relationships and Managing Risk are core themes taught within PSHE lessons in all year groups.
- Key events on the school calendar – Safer Internet Day, Anti-Bullying Week – are addressed through whole school assemblies and form time LEARN sessions.
- Students are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. This includes making clear the correct use of ICT in accordance with exam board regulations in Y10 and above.
- Students are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making, both through PSHE and individual subject lessons.
- Students are helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- In lessons where internet use is pre-planned students will be guided to sites checked as suitable for their use.
- Where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that may result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study, particularly with regard to the age and stage of the students involved.

6) Wider education and training of stakeholders

Parents / Carers:
The school will seek to provide information and awareness to parents and carers through:

- Information signposted on our school website
- Letters, newsletters, booklets (e.g. Digital Parenting), emails
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers
- The provision of training packages via our membership with National Online Safety.

Staff / Governors/Volunteers:

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be accessed as follows:

- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff annually as part of the whole school CPD programme.
- This Online Safety Policy and its updates will be presented to and discussed by governors annually as part of the review cycle. Additional training for governors will be signposted.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.
- The provision of training packages will be signposted via our membership with National Online Safety.

7) Technical – infrastructure / equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will be provided with a username and secure password by the network manage who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be advised to change their password on a regular basis
- Internet access is filtered for all users. Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.

8) Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet.

Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment and only kept on school IT storage systems; they must not be taken home or transferred onto a personal portable/device or emailed to personal email addresses. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs, without parental consent.
- Student's work can only be published with the permission of the student and parents or carers.

9) Data Protection: The Data Protection Act 2018 **controls how your personal information is used by organisations, businesses or the government**. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 (updated 2018) which states that personal data must be:

- Fairly and lawfully processed
- Processed for specific, explicit limited purposes
- Adequate, relevant, limited and not excessive to only what is necessary
- Accurate and up to date
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Safe and secure
- Only transferred to others with adequate protection. Not to be transferred outside the EEA

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Lock computers even if briefly leaving the room for any reason and if the computer will be unattended for a period of time in an environment where others may view the screen or gain access to data.

10) Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how our permissions for both staff and students.

	Staff			Students		
Communication Technologies	Allowed	Allowed for certain education purposes	Not allowed	Allowed	Allowed with approval	Not allowed
Mobile phones may be brought to the school	■			■		
Use of mobile phones in lessons		■			■	
Use of mobile phones in social time	■					
Taking photos on own mobile phones		■			■	
Taking photos on a school camera	■				■	
Use of other mobile devices e.g. tablets, gaming devices		■			■	
Use of personal email addresses to send emails in school			■			■
Use of school email addresses for non-school use			■			■
Use of messaging apps in school	■					
Use of social media in school		■				

* SLT approves the use of mobile phones in lessons according to the following protocols:

- The use of mobile phones must support learning in a clear and recognisable way. This could include:
    - Providing a backing track to sing to in Music
    - Searching for artwork as inspiration in an Art lesson
    - Playing a Kahoot quiz to embed knowledge in any lesson
    - Creation of a school-based video presentation (e.g. for Awards Evening)

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the DSL – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, Teams etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

11) Social Media - Protecting Professional Identity:

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through ensuring that personal information is not published.

School staff should ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites

12) Remote Learning

The increase in remote learning as a result of Coronavirus has meant that teachers must be aware of additional measures which include:

- The use of the waiting lobby is set as standard for each lesson so a teacher must not allow a user to enter if (a) it is an unrecognised name and (b) it has the word Guest underneath it. Such an incident must be passed on to the IT Support team or Online Safety Lead.
- The teacher should be the only presenter in a Team (again, set as standard). If a pupil wishes to be unmuted then they can raise their hand for this to be facilitated.
- Teachers should be as vigilant as would be expected in a normal classroom with regard to poor behaviour and resolve this through the usual channels.

13) Unsuitable / inappropriate activities:

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X

	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	X
	threatening behaviour, including promotion of physical violence or mental harm				X	X
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	X
Creating or propagating computer viruses or other harmful files						X
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)					X	
On-line gambling					X	X*
On-line shopping / commerce			X			
File sharing			X			
Use of social media			X			
Use of messaging apps			X			

Use of video broadcasting e.g. YouTube			X		

* = student use only

14) Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents:

In the case of suspected illegal incidents, the information should be passed on to the Headteacher who will forward further information to the DSL. Contact will also be made with the police, parents and any other external body as deemed appropriate, in line with school disciplinary procedures.

Other Incidents:

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- The DSL and Network Manager should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by external agencies
    - Police involvement and/or action if required

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately through liaison with the DSL. Staff should not ask to view, store or share images – advice should be sought as soon as possible.
- Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material

    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

15) School Actions & Sanctions:
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with in line Respect to Learn (R2L policy) and Staff Code of Conduct.

16) Vulnerable Learners
Many vulnerable children are also those most at risk online; in addition to the harm that this does, it also reduces their opportunity to flourish within the online environment they may find preferable. Over 2 million children in England are living in families with complex needs. Many children are living in families with domestic abuse, parental substance abuse and mental health problems.

Westhoughton High School recognises that some learners are more vulnerable due to a range of factors. Those children may be:

- Receiving statutory care or support.
- Known to have experienced specific personal harm.
- With a disability, ill-health or developmental difficulties.
- In households or families with characteristics or locations that indicate higher potential likelihood of current and future harm.
- Vulnerable or of concern by virtue of their identity or nationality.
- At risk in relation to activity or institutions outside the home.
- Caring for others.

Westhoughton High School will ensure the effective and safe provision of tailored online safety education. Westhoughton High School will obtain input and advice from specialist staff as deemed necessary.