Wellbrook School: Online Safety Policy

Complied:	August 2024
Reviewed by:	C. Howells
Last Review Date:	March 2025
Approved by:	Governance Committee
Approval Date:	March 2025
Next Review date:	March 2026
Version Number:	Version 2
Policy Number:	21

Introduction

At Wellbrook School, we strive to provide every child with the opportunity to unlock their potential. We honour and celebrate their individuality and tailor our instruction to their personal needs. Our goal is to nurture self-confidence and provide students with the support necessary to help them reach heights they didn't think were possible. We want parents to imagine the possibilities when they walk through our doors and be filled with hope as they see their children achieve beyond their expectations. We strive to be a place where children feel they belong and can thrive.

Our school is also committed to safeguarding and promoting the welfare of all its pupils including protecting them from online threats. This policy outlines the steps we will take to safeguard our pupils from online threats.

Note:

- the terms 'child' or 'children' apply to anyone under the age of 18
- the term 'parent' applies to anyone with guardianship or caring and parental responsibility for the child
- the term 'staff' applies to members of staff and volunteers

Our online safety statement:

This policy provides guidance on how our school uses the internet and social media, and the procedures for doing so. It also outlines how we expect the staff who work for us, and the children who are members of our school, to behave online. As a school, we commit to implementing this policy and addressing any concerns quickly and within these guidelines.

The aims of our online safety policy are:

- to protect all children at our school who make use of technology (such as mobiles phones, games consoles and the internet) while in our care
- to provide staff with policy and procedure information regarding online safety and inform them how to respond to incidents
- to ensure our school is operating in line with our values and within the law regarding how we behave online

Understanding the online world

As part of using the internet and social media, our school will:

- assess and manage the safety aspects – including what is acceptable and unacceptable behaviour for staff and children when using websites, social media including Facebook, TikTok, Instagram, Twitter, Snapchat, other apps, and video conferencing platforms including Teams, Zoom or Skype
- be aware of how staff in our school and the children they work with use social media both inside and outside of our setting
- ensure that we adhere to relevant legislation and good practice guidelines when using social media or video conferencing platforms
- provide training for the staff responsible for managing our school's online presence
- provide relevant training for all staff, school leaders, members of the governance committee , and the proprietor
- teach pupils how to stay safe online
- regularly review existing safeguarding policies and procedures to ensure that online safeguarding issues are fully integrated, including:
  - making sure concerns of abuse or disclosures that take place online are written into our reporting procedures
  - incorporating online bullying ('cyberbullying') in our anti-bullying policy

Managing our online presence

Our online presence through our website or social media platforms will adhere to the following guidelines:

- all social media accounts will be password-protected, and at least 2 members of staff will have access to each account and password
- each account will be monitored by at least two designated members of staff in order to provide transparency
- the designated staff managing our online presence will seek advice from our designated safeguarding lead to advise on safeguarding requirements
- designated staff will remove inappropriate posts by children or staff, explaining why, and informing anyone who may be affected (as well as the parents of any children involved)
- we'll make sure children are aware of who manages our social media accounts and who to contact if they have any concerns about something that's happened online,

- our account, page and event settings will be set to 'private' so that only invited members can see their content
- identifying details such as a child's home address, school name or telephone number shouldn't be posted on social media platforms
- any posts or correspondence will be consistent with our aims and tone as a school
- parents will be asked to give their approval for us to communicate with their children through social media, via video conferencing platforms or by any other means of communication
- parents will need to give permission for photographs or videos of their child to be posted on social media
- video conferencing sessions will be password protected in order to maintain children's privacy and prevent exposure to inappropriate or harmful content by third parties

Appropriate Filtering and Monitoring

- Our computer networks have appropriate filtering (appendix 1) and monitoring (appendix 2) according to the guidance provided by the UK Safer Internet Centre, The school have implemented Smoothwall for their filtering and monitoring, alerting both the DSL and DDLS/Headteacher to any concerns.

- We will ask the provider who manages our computer networks to self-certify that they meet the standards by completing the UK Safer Internet Centre's checklists for appropriate filtering and monitoring and forwarding them on for publishing on their website

- **All staff at our school** - will receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring during induction.

- **The designated safeguarding lead** - will take lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place. They will also complete training to help them understand filtering and monitoring such as UK Safer Internet's webinar "Filtering and Monitoring, and Introduction" and training which explores what those responsible for safeguarding need to consider regarding filtering and monitoring systems, as part of a school or college's overarching safeguarding approach. UK Safer Internet have a suitable cause titled "Responsible for Safeguarding". The Designated Safeguarding Lead will consult those who manage the school's filtering and

monitoring systems to get a better understanding of the processes in place at the school.

- **The proprietor and members of the governance committee** - will complete training to help them understand filtering and monitoring such as the UK Safer Internet's webinar "Filtering and Monitoring, and Introduction". In addition to that they will also complete training which explores what those responsible for safeguarding need to consider regarding filtering and monitoring systems, as part of a school or college's overarching safeguarding approach. UK Safer Internet have a suitable cause titled "Responsible for Safeguarding" The proprietor and members of the governance committee are responsible for ensuring that all staff receive appropriate safeguarding and child protection training and updates (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.

- **Filtering & Monitoring Standards** – Our members of the governance committee , the proprietor, DSL and the SLT responsible for filtering and monitoring will read and understand the filtering and monitoring standards for schools and colleges. UK Safer Internet have a suitable course titled "An Overview of New Filtering and Monitoring Standards" which can be found here: https://swgfl.org.uk/resources/filtering-and-monitoring/. The SLT responsible for filtering and monitoring, the DSL and the school's IT service provider will evaluate the school's compliance with the filtering and monitoring standards. UK Safer Internet have compiled a helpful checklist which can be download here: https://swgfl.org.uk/resources/filtering-and-monitoring/. The school will implement any actions required to address non-compliance identified then put in place measures to ensure that compliance is maintained.

- **Cyber Security Standards** - Our members of the governance committee , the proprietor, DSL and the SLT responsible for filtering and monitoring will read and understand the cyber-security standards for schools and colleges The SLT responsible for filtering and monitoring, the DSL and the school's IT service provider will evaluate the school's compliance with the cyber security standards. School leaders and staff will complete the National Cyber Security Centre's (NCSC) training titled "Cyber Security Training for School Staff"

What we expect of our staff

- staff should be aware of this policy and behave in accordance with it
- staff should seek the advice of the designated safeguarding lead if they have any concerns about the use of the internet or social media
- staff should communicate any messages they wish to send out to children to the designated staff responsible for the school's online presence
- staff should not communicate with children via personal accounts
- staff should not 'friend' or 'follow' children from personal accounts on social media and they should maintain the same professional boundaries online as they would in person when using school accounts
- staff should make sure any content posted on public personal accounts is accurate and appropriate, as children may 'follow' them on social media
- rather than communicating with parents through personal social media accounts, staff should choose a more formal means of communication, such as face-to-face, in an email or in writing, or use a school account or website
- staff should avoid communicating with children via email or school social media outside of normal office hours
- emails or messages should maintain the school's tone and be written in a professional manner, e.g., in the same way you would communicate with fellow professionals, **avoiding kisses (X's) or using slang or inappropriate language**
- staff should not delete any messages or communications sent to or from school accounts
- staff should undertake all online safety training offered and gain a basic knowledge of the platforms children use and how to report or remove inappropriate content online
- any concerns reported through social media should be dealt with in the same way as a face-to-face disclosure,
- according to our reporting procedures at least one parent must be present during the delivery of any activities via video conferencing platforms at home (refer to the Remote Learning Policy)
- any delivery of activities to children via video conferencing platforms will be supported by an additional member of staff (even if they're not actively delivering) to ensure transparency
- staff and children **must not** engage in 'sexting' or send pictures to anyone that are obscene

What we expect of children

- children should be aware of this online safety policy and agree to its terms
- we expect children's behaviour online to be consistent with the guidelines set out in our acceptable use statement
- children should follow the guidelines set out in our acceptable use statement (appendix 3) on all digital devices, including smart phones, tablets, and consoles

What we expect of parents

- parents should be aware of this online safety policy and agree to its terms
- parents should protect all children's privacy online and think carefully about what content they share about our school online, where they share it and who they're sharing it with
- we expect parents' behaviour online to be consistent with the guidelines set out in our acceptable use statement (appendix 3) and in our codes of conduct for parents and spectators

Using mobile phones or other digital technology to communicate

When using mobile phones (or other devices) to communicate by voice, video, or text (including texting, email, and instant messaging such as WhatsApp or Facebook Messenger), we'll take the following precautions to ensure children's safety:

- staff will avoid having children's personal mobile numbers and will instead seek contact through a parent
- we'll seek parental permission on each occasion we need to contact children directly; the purpose for each contact will be clearly identified and agreed upon
- a method of accountability will be arranged, such as copies of texts, messages or emails also being sent to another member of staff or to parents
- smartphone users should respect the private lives of others and not take or distribute pictures of other people if it could invade their privacy
- staff should have a separate phone from their personal one for any contact with parents or children
- texts, emails, or messages will be used for communicating information – such as reminding children or young people about upcoming events, which kit to bring or practice timings – and not to engage in conversation if a child misinterprets such communication and tries to engage a staff member in conversation, the member of staff will take the following steps:

- o   end the conversation or stop replying
- o   suggest discussing the subject further at the next practice or event
- o   inform the schools lead safeguarding officer in the interest of transparency
- if concerned about the child, provide contact details for the schools designated safeguarding lead or appropriate agencies, and report any concerns using the schools reporting procedures

Using mobile phones

- At Wellbrook school, we are committed to establishing and maintaining high standards of behaviour, minimising disruption to learning and ensuring that the school is a calm and safe environment for all pupils and staff. To that end, we do not permit pupils to use mobile phones and similar devices throughout the school day, including during lessons, the time between lessons, breaktimes, lunchtimes and during sports activities. For this reason:
  - o   pupils will be asked to hand in their mobile phones to staff upon arrival at school
  - o   mobile phones will be kept in a secure location until the end of the school day
- Details about how this will be implemented can be found in the school's Mobile Phone Policy.

Further information for parents about keeping children safe online

- NSPCC The NSPCC's guidance for parents on online safety nspcc.org.uk/keeping-children-safe/online-safety
- Child Exploitation and Online Protection Centre (CEOP) Child Exploitation and Online Protection Demand's website ceop.police.uk
- The UK Safer Internet Centre Safer Internet Centre's advice for parents and children saferinternet.org.uk

Appendix 1: UK Safer Internet Centre – Appropriate Filtering

Guide for education settings and filtering providers about establishing 'appropriate levels of filtering'

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". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England 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." Ofsted concluded in 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems". Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves."

The aim of this document is to help education settings (including Early years, schools, and FE) and filtering providers comprehend what should be considered as 'appropriate filtering'.

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.

Illegal Online Content

In considering filtering providers or systems, schools should ensure that access to illegal content is blocked, specifically that the filtering providers:

- Are IWF members and block access to illegal Child Sexual Abuse Material (CSAM)
- Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, schools should be satisfied that their filtering system manages the following content (and web search):

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances
- Extremism: promotes terrorism and terrorist ideologies, violence, or intolerance
- Malware / Hacking promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography: displays sexual acts or explicit images
- Piracy and copyright theft includes illegal provision of copyrighted material
- Self-Harm: promotes or displays deliberate self-harm (including suicide and eating disorders)
- Violence: Displays or promotes the use of physical force intended to hurt or kill
- This list should not be considered exhaustive, and providers will be able to demonstrate how their system manages this content and many other aspects

Regarding the retention of logfile (Internet history), schools should be clear about the data retention policy of their provider.

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

Filtering System Features

Additionally, schools should consider that their filtering system meets the following principles:

- Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role

- Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services and DNS over HTTPS

- Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content

- Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking

- Group/Multi-site Management – the ability for deployment of central policy and central oversight or dashboard

- Identification - the filtering system should have the ability to identify users

- Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)?
- Multiple language support – the ability for the system to manage relevant languages
- Network level - filtering should be applied at 'network level' i.e., not reliant on any software on user devices
- Reporting mechanism – the ability to report inappropriate content for access or blocking
- Reports – the system offers clear historical information on the websites visited by your users

Schools and Colleges should ensure that there is sufficient capability and capacity in those responsible for and those managing the filtering system. The UK Safer Internet Centre Helpline may be a source of support for schools looking for further advice in this regard.

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". To assist schools and colleges in shaping an effective curriculum, UKCCIS have published Education for a Connected World.

We will ask our Filtering and Monitoring provider with the Safer Internet UK Filtering Checklist: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/provider-checklists

We will ask them to complete all fields and return the form to UK Safer Internet Centre (enquiries@saferinternet.org.uk), to illustrate how their particular technology system(s) meets the national defined standards.

Appendix 2: UK Safer Internet Centre – Appropriate Monitoring

Guide for education settings and filtering providers about establishing 'appropriate levels of monitoring'

Schools (and registered childcare providers) 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". Furthermore, it expects that they "assess the risk of [their] children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology". There are a number of self-review systems (such as 360 degree safe) that will support a school in assessing their wider online safety policy and practice.

The Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England 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."

Supplementary to the risk assessment above, UK Safer Internet Centre recommends that Schools and Colleges further assess their broader online safety provision that includes filtering (and monitoring) provision. The risk assessment should consider the risks that both children and staff may encounter online, together with associated mitigating actions and activities. A risk assessment module has recently been integrated in 360 degree safe. Here schools can consider, identify, and record the risks posed by technology and the internet to their school, children, staff, and parents.

The aim of this document is to help schools (and providers) comprehend, in conjunction with their completed risk assessment, what should be considered as 'appropriate' monitoring.

Monitoring Strategies

There are a range of monitoring strategies and systems, however the appropriate monitoring strategy selected should be informed by your risk assessment and

circumstances. It is also vitally important to review and refine the relevant policies as part of assessing (or implementing) a monitoring strategy or system.

The following are examples.

1) Physical Monitoring

Most suited where circumstances and the assessment suggests low risk. This could be physical supervision of children while using the Internet; assigning additional classroom support staff to monitor screen activity; or actively monitoring all screen activity during a lesson from a central console using appropriate technology.

The following are possible limitations or points to consider:

- Can be resource intensive
- Less effective across a larger group or a group using mobile devices
- Pupils often adapt screen behaviour to avoid monitoring
- Advantage of immediate intervention when an issue arises which can be developed as a teaching opportunity

2) Internet and web access

Some Internet Service Providers (ISPs) or filtering providers provide logfile information that details and attributes website access and search term usage against individuals. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches.

The following are possible limitations or points to consider:

- Assign appropriate responsibility for analysing the logfile information. These reports can often be difficult to understand and may require specialism to analyse.
- The frequency that blocks or monitoring lists are updated by your provider
- The logfile information should be able to identify an individual user (or group as appropriate) for effective intervention
- Logs need to be regularly reviewed, interpreted and alerts prioritised for intervention
- Information held by the school that indicates potential harm, must be acted upon

● Be aware of any limitations of the logfile information

3) Active/Proactive technology monitoring services

Where the risk is assessed as higher, Active or Proactive monitoring technologies may be suitable. These specialist services provide technology-based monitoring systems that actively monitor use through keywords and other indicators across devices. These can prove particularly effective in drawing attention to concerning behaviours, communications, or access.

These systems can take the form of:

● Active monitoring where a system generates alerts for the school to act upon
● Proactive monitoring where alerts are managed by a third-party provider and may offer support with intervention.

The following are possible limitations or points to consider

● Can be expensive in terms of installing and maintaining technology
● Proactive monitoring uses specialist organisations and may involve additional expense
● Active monitoring requires sufficient internal capability and capacity
● Active monitoring can initially generate significant volumes of information and alerts which can be difficult to interrogate and interpret.
● Assign appropriate Safeguarding expertise to review, prioritise, and take action on alerts that signal potential harm

Monitoring Content

Recognising that no monitoring can guarantee to be 100% effective, schools should be satisfied that their monitoring strategy or system (including keywords if using technical monitoring services) at least covers the following content:

● Illegal: content that is illegal, for example child abuse images and terrorist content

● Bullying: Involve the repeated use of force, threat, or coercion to abuse, intimidate or aggressively dominate others

● Child Sexual Exploitation: Is encouraging the child into a coercive/manipulative sexual relationship. This may include encouragement to meet.

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010

- Drugs/substance abuse displays or promotes the illegal use of drugs or substances

- Extremism: promotes terrorism and terrorist ideologies, violence, or intolerance

- Pornography: displays sexual acts or explicit images

- Self-Harm: promotes or displays deliberate self-harm

- Violence: Displays or promotes the use of physical force intended to hurt or kill

- Suicide: Suggests the user is considering suicide

Monitoring Strategy/System Features

Schools should consider how their system integrates within their policies (see templates) and should satisfy themselves that their monitoring strategy meets the following principles:

- Age appropriate – includes the ability to implement variable monitoring appropriate to age. This will in turn define which alerts are prioritised and responded to. Further situations may warrant additional capability, for examples boarding schools or community-based access

- BYOD (Bring Your Own Device) – if the system includes the capability to monitor personal mobile and app technologies (i.e., not owned by the school), ensure it is deployed and supported and how data is managed. Does it monitor beyond the school hours and location?

- Data retention – should be clear what data is stored, where and for how long

- Devices – if software is required to be installed on devices, the monitoring system should be clear about the devices (and operating systems) it covers

- Flexibility - changes in keywords (addition or subtraction) can be easily according to an agreed policy

- Group/Multi-site Management – the ability for deployment of central policy and central oversight or dashboard

- Impact - How do monitoring results inform your policy and practice?

- Monitoring Policy – How are all users made aware that their online access is being monitored? How are expectations of appropriate use communicated and agreed? Does the technology provider offer any advice or guidance?

- Multiple language support – the ability for the system to manage relevant languages

- Prioritisation – How alerts generated via monitoring are prioritised to enable a rapid response to immediate issues. What operational procedures are in place to facilitate that process?

- Reporting – how alerts are recorded, communicated, and escalated?

Monitoring systems require capable and competent staff with sufficient capacity to effectively manage them, together with the support and knowledge of the entire staff. Monitoring systems are there to safeguard children and the responsibility therefore should lie with the school leadership/members of the governance committee and Designated Safeguarding Lead. Schools and Colleges should ensure that there is sufficient capability and capacity in those responsible for and those managing the filtering system. The UK Safer Internet Centre Helpline may be a source of support for schools looking for further advice in this regard.

We will ask our Filtering and Monitoring provider with the Safer Internet UK Monitoring Checklist: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/provider-checklists

We will ask them to complete all fields and return the form to UK Safer Internet Centre (enquiries@saferinternet.org.uk), to illustrate how their particular technology system(s) meets the national defined standards.

Appendix 3: Statement of Acceptable Use of Internet and Social Media

Wellbrook School understands the importance of online communication for children's and young people's development. However, we recognise that relevant safeguards need to be put in place to ensure children and young people remain safe while online or using social media.

We ask that all parents / carers spend a few minutes to read through and discuss this statement with their child and then sign and return this form to Wellbrook School's Designated Safeguarding Lead – S. Hughes

*Agreement of child / young person

1. I will be responsible for my behaviour when using my phone at the school, including the content I access and how I conduct myself.

2. I will not deliberately create, browse, or access material that could be considered offensive or illegal. If I accidentally come across any such material, I will report this to a member of staff.

3. I will not use social media or the internet to send anyone material that could be considered threatening, offensive, upsetting, bullying or that is illegal.

4. I understand that I should only use the school's official social media or website communication channels to contact them and should not seek out individual members of staff.

5. I understand that all my use of the internet and social media is potentially visible to everyone and that any issues involving my behaviour online may be addressed by my teachers or other staff members at the club.

6. I will not give out any of my personal information (such as name, age, address, or telephone number) online, or that of anyone else.

7. I will not share my passwords with anyone else.

8. I will not arrange to meet someone that I have met online unless accompanied by a member of staff or parent.

9. I understand that these rules are designed to keep me safe, and if they are not followed my parents may be contacted.

10. I will avoid using my mobile phone during activities as I understand that it will have an impact on my safety and my opportunity to learn and achieve.

11. I am aware that if I am experiencing bullying behaviour or abuse online, I can contact S. Hughes.

12. I know I can contact Childline on **0800 11 11** or at **childline.org.uk** if I have any worries about something I've seen or experienced online.

Declaration – parent / carer	
We have discussed this statement and *(print child's name)* -- agrees to support the safe use of the internet and social media at **Wellbrook School**.	
Signature	✘
Print name	
Today's date	

Declaration – child / young person	
Signature	✘
Print name	
Today's date	