Brockwood Park School

BROCKWOOD PARK SCHOOL

E-SAFETY POLICY

Last Review Date	August 2024
Policy endorsed by	The Trustees and School Management Committee
Policy is maintained by	DSL and SMC (IT Liaison)
Next review date	August 2025
Review body	School Management Committee and DSL

Table of contents

1. Introduction **2**
2. Aims and Objectives **2**
3. Scope **3**
4. Role and Responsibilities **3**
Trustees 3
Co-Chairs 4
Designated Safeguarding Lead (DSL) 4
IT Administration Team 5
All staff, volunteers and guests 5
5. E-Safety Education **6**
6. Cyberbullying **8**
7. Security and Management of Information Systems **8**
Reducing online risks 8
Firewall and protection software 9
8. Incidents and response **10**
9. Training **10**
10. Monitoring arrangements **10**

1. Introduction

Brockwood Park School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff, and encourage the use of computers in both teaching and learning. Any user of the school IT system must adhere to the Acceptable Use Agreement. However, the accessibility and global nature of the internet and mobile phone technology mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies and IT education for students. In furtherance of our duty to safeguard students, we will do all that we can to enable our students and staff to stay e-safe and to satisfy our wider duty of care.

2. Aims and Objectives

The school aims to have an effective approach to online safety to safeguard everyone from potentially harmful and inappropriate online material, and to educate students and staff in their use of technology that establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The aims of this policy are:

- safeguard and protect all members of the school online
- identify approaches to educate and raise awareness of online safety throughout the school
- enable staff and students to work safely and responsibly and to maintain professional standards and practice when using technology; and
- identify clear procedures to use when responding to digital safety concerns.

Brockwood Park School recognises that the breadth of risk within online safety is considerable and ever evolving, but can be categorised into four areas of risk as per the latest KCSIE September 2024:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Scope

The policy applies to all members of the school community who have access to the IT system, both on the premises and remotely. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as e-mail, mobile phones and social media sites. The impact of the policy will be monitored regularly with a full review being carried out at least once a year. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

4. Role and Responsibilities

Trustees

The Trustees have overall responsibility for monitoring this policy and holding the DSL to account for its implementation.

They make sure they are up to date with the DfE filtering and monitoring standards, and discuss with relevant staff to ensure the school meet those standards which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Trustees will:

- Ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Make sure all staff undergo online safety training as part of child protection and safeguarding training, and that staff understand their expectations, roles and responsibilities around filtering and monitoring.
- Make sure that all staff receive regular online safety updates (via email, training or staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

- Coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- Ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.

Co-Chairs

Brockwood Park School is run by a management committee, currently consisting of the following four members: Kate Power, Mina Masoumian, Thomas Lehmann and Tom Power. The School Management Committee (SMC) is overseen and coordinated by two Co-Chairs: Mina Masoumian and Thomas Lehmann.

The SMC fulfils the role of a Principal/Headteacher in the school. From the safeguarding perspective and for any reference made to Principal/Headteacher in the standards and KCSIE (Keeping Children Safe in Education), this role is fulfilled by the Co-Chairs. One of the Co-Chairs is the DSL.

The Co-Chairs (one of whom is a DSL) are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Designated Safeguarding Lead (DSL)

Details of the school's DSL and DDSLs are set out in our child protection and safeguarding policy, as well as relevant job descriptions. The School's DSL is one of the Co-Chairs of the School Management Committee.

The DSL takes lead responsibility for online safety in school, in particular:

- Working closely with the other Co-Chair to ensure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the other Co-Chair and with the Trustees to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the IT Administration team to make sure the appropriate systems and processes are in place
- Working with the pastoral team, IT Administration team and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (online safety incident report log) and dealt with appropriately in line with this policy and the school's child protection and safeguarding policy

- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Working closely with the IT Administration team to update and deliver staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the other Co-Chair and Trustees
- Undertaking annual risk assessments that consider and reflect the risks children face
- Including online safety in regular safeguarding and child protection updates given to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Including online safety in regular safeguarding updates given to Trustees in each Trustee Meeting (three times a year)

IT Administration Team

The IT Administration Team is comprised of the SMC IT Liaison, who is currently Tom Power, Intech IT Solutions who action decisions made by the School Management Committee (SMC), and the school IT Administrator, Julian Mardelet, who works closely with the SMC and Intech to keep the IT provision working and safe. This team is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy
- Building a positive technology culture in school by facilitating students and all members of the community in developing wise use of technology. As part of this, internet access is switched off during mealtimes

All staff, volunteers and guests

All, staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet as stated in the Code of Conduct (Use of IT including social media) and ensuring that students follow the school's terms on acceptable use as stated in the ICT Acceptable Use Student Agreement 2024-25.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by completing the Safeguarding Concern Form available in the school (copies of these forms can be found in the Reception of Brockwood, Pastoral Office at Brockwood, the staff office at Inwoods or can be obtained from the DSL).
- Following the correct procedures by seeking permission from the DSL or one of the Co-Chairs if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

Guests and visitors to the school will be able to access the internet via our 'Guests' SSID. Access to this network can be given for specific periods of time depending on their need. The school secretary can create access codes for different lengths of time as agreed with each guest. All internet traffic through our Guests network is filtered and monitored and guests and visitors are informed of this via the guidance on their visitors badge. Guests are expected to use the internet in an appropriate way while connected to the Guests network.

5. E-Safety Education

Students are taught about online safety as part of the school's PSHE programme; below are some of the points covered:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks including any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online:
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content and being subject to harmful interaction with other uses
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- Importance of using strong passwords so as to prevent their accounts from being compromised. Awareness around MFA (Multi Factor Authentication) to prevent unauthorised access. Understand the risk involved in using Public WIFI spots where security and encryption is not guaranteed. Emails requesting details of passwords (especially for sensitive information such as bank details) are certainly 'phishing' and should be deleted and/or reported to the organisation from which they purport to come.
- Importance of understanding the addictive nature of technology and its impact on attention spans and health.
- Understanding the impact of social media
- Impact of using the DarkNet
- Impact of online gaming

The school endeavours to develop critical thinking skills so that students feel empowered to evaluate the reliability and purpose of information online, rather than accepting everything at face value. This will involve asking questions, checking a variety of sources, researching the origins of information and forming their own opinions and judgements. Although the school does not specifically ban AI powered programs like ChatGPT we endeavour to make students aware of the advantages and disadvantages of using such programs.

6. Cyberbullying

Please refer to the school's *Anti-Bullying Policy*.

7. Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Providing encryption functionality for staff for personal data sent over the internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
- Not using portable media without specific permission; portable media can be checked by staff using an antivirus/malware scan before use
- Configuring the ICT estate to prevent the downloading of unapproved software to work devices or opening unfamiliar email attachments
- Implementing anti-virus and anti-spam systems on our email system
- Virus protection being updated regularly
- The ability to check files held on our network as required
- The appropriate use of user logins, passwords and best security practices such as multi-factor authentication to access our network.
- All users are asked and expected to log off or lock their screens/devices if systems are unattended.
- Specific user logins and passwords enforced for all
- Applying appropriate access for staff to data stored on School systems.

Reducing online risks

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the School's computers or devices. However, the school:

- Regularly reviews the methods and tools used to identify, assess and minimise online risks
- Examines emerging technologies for educational benefit and undertake appropriate risk assessments before use in the School is permitted
- Ensures that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material

Students at Brockwood Park have access to their phones on Saturdays from 7am to 7pm. During this time the school will provide filtered and monitored internet access via the Student WIFI network. We cannot take responsibility if students access the internet via their mobile service provider and so insist that students use the Students WIFI network to access the internet as a condition of having their phone on Saturdays.

Firewall and protection software

Levels of internet access are adjusted according to time of day and to allow for greater freedom when browsing outside of class time and during the weekends. The School uses firewall services from SOPHOS to implement filtering and to protect the Schools' network from cyber threats. Filtering is done on the basis of content, URL keywords and category. The categories are updated by the DSL/DDSL via Fastvue. We use SSL inspection for specific keywords which indicate harmful content. Internet filtering categories (which define what sites and services are allowed or blocked) are defined by the School Management Committee and the IT Administration Team. They have considered the DfE and other regulatory guidance. These are reviewed annually before the start of each academic year and in consultation with the provider.

Monitoring is done at different levels:

- Physical where the staff members monitor use of computers during specific days and timings. Students are required to mention the time and place where they will be using a device in the school.
- Internet browsing history and web logs are maintained for each student and can be examined if the software raises an alert. The school uses Fastvue for monitoring. Fastvue has been configured with tools such as web filters and SSL inspection so that appropriate alerts are raised along with audit details which allows the management of any incident efficiently. Real time activity can also be monitored and this is done keeping in mind the privacy rights of students. All our school computers have fixed IPs and activities on these computers are logged. We also have individual logins for students so that we can monitor how much time a student spends on the computer and what content is being viewed. The reports produced by Fastvue specify what sites were blocked, when and on which computer and user. These are checked by the DSL every two weeks or more frequently depending on the level of concern and are reported for further action.
- The school uses the G Suite Mobile Device Management Policy to ensure that all Mobile devices are monitored and students are required to download the policy to ensure data protection. The software also provides wide ranging reports on bandwidth usage and details of which sites and hosts were flagged or blocked along with the date and time.
- Parents at Brockwood are informed via our Use of ICT Mobile Phones and Electronic Devices Policy to cooperate and install a content filtering app on their child's devices to make sure no inappropriate content can be accessed even when using 3G/4G/5G.

8. Incidents and response

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our *Safeguarding and Child Protection Policy* and *Behaviour of Students Policy*. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The DSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns and will record these issues in line with our Safeguarding and Child Protection policies. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Hampshire Safeguarding Children's Board thresholds and procedures. The DSL will inform parents of online safety incidents or concerns involving their child, as and when required.

9. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation.

All staff members and volunteers will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (through emails, training and staff meetings).

The DSL and DDSLs will undertake in-depth child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

10. Monitoring arrangements

Technology in this area evolves and changes rapidly, so this policy will be reviewed on an annual basis. The policy will also be revised following any local or national changes to policy and procedure, any child protection concerns and/or changes to the School's technical infrastructure. Internet use is always recorded and regularly monitored, and we will continue to evaluate the School's digital safety mechanisms to ensure this policy is consistently applied. The DSL will be informed of digital safety concerns, as appropriate. The DSL will report to the Board of Trustees on online safety practice and incidents, including outcomes, on a regular basis. Any issues identified via monitoring will inform our action planning.

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL and the other Co-Chair of the SMC and SMC IT Liaison At every review, the policy will be shared with the Trustees. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.