ICT USE, Technology, e-SAFETY AND COOKIE POLICY

INWOODS SMALL SCHOOL

Last Review Date	August 2023
Policy endorsed by	The Trustees and School Management Committee
Policy is maintained by	IT Administrator / Inwoods Coordinator / DSL
ISI reference	A6, B1, B9, A8, A9
Next review date	August 2024
Review body	School Coordinator and Co-chairs

This policy applies to all staff and students and anyone using the school internet system.

Reporting Incidents

Should an e-safety incident occur please contact: Mina Masoumian: Designated Safeguarding Lead (DSL) at Brockwood and Inwoods, or Kate Power, the coordinator at Inwoods and the Deputy Designated Safeguarding Lead (DDSL). Lauren Bradshaw is also a Deputy Designated Safeguarding Lead (DDSL) at Inwoods Small School. If none of the team can be contacted and you believe a child to be in danger of serious and imminent harm then please contact: Children's Services: **0300 555 1384**

Introduction

Inwoods Small School is dedicated to nurturing each child's capacity for creative imagination, independent thinking and positive action. We value learning experiences that are experiential and hands-on. With this in mind we think carefully about using screens in the classroom spaces. There is no direct computer and internet access for younger children and limited access for Year 5 and Year 6 children. The occasional use of screens as a tool might occur, such as the use of tablets to take pictures of their work and very occasionally we might use a laptop to show something related to the topic we are teaching that we can't show on a piece of paper or in the learning environment outside. At times, we might use a projector to look at an image on a larger scale, which we feel would really inspire the children or help them to understand it in more detail. But as a clear intention there is consideration for the role of technology within our curriculum from Year 1 to Year 6 and having the classrooms as screen free as possible.

When computer access is allowed 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 the children. In furtherance of our duty to safeguard, we will do all that we can to enable our pupils and staff to stay e-safe and to satisfy our wider duty of care.

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 and establish 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.

Inwoods Small 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 2023:

- 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

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.

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 governing board 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.
- Co-ordinate regular meetings with DSL 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

Inwoods Small Small is a junior school to Brockwood Park School and both schools are overseen 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 coordinator 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 schools.

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 Administrator to make sure the appropriate systems and processes are in place
- Working with the other teachers, IT Administrator 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 cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Working closely with the IT Administrator 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 Administrator

The IT Administrator 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 cyber-bullying are dealt with appropriately in line with the school behaviour policy

All staff and volunteers

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)
- 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 (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying 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'

Access to the Internet

At Inwoods Year 5 and 6 children are allowed limited internet access in school at the discretion of the teacher. We recognize that being computer literate is essential in our current society and so it is important for the children that they have these skills when they leave Inwoods. We are aware that some children will have access to such technologies at home by this age.

The use of the internet can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism, as well as access to unsuitable video / internet games.
- Inappropriate contact: 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 being subjected to harmful online interaction with other users.
- Inappropriate communication /conduct, for example, making, sending and receiving explicit images, such as consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying. The sharing / distribution of personal images without an individual's consent or knowledge.
- Commerce risks such as online gambling, inappropriate advertising, phishing and or financial scams. Unauthorised access to / loss of / sharing of personal information. Illegal downloading of music or video files.

When children are using computers, they are to be seated in areas of high visibility which will enable children, young people and adults to be closely supervised and their online use to be appropriately monitored.

E- Safety Education

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Staff, alongside parents and carers, should consider it to be their duty to make children and young people aware of the potential risks, as well as benefits, associated with online technologies. This will empower them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

In the project work across the key stages references to technology will be made. This could be references to technology that they encounter in daily life, such as cars, mobile phones and cameras. The children will have conceptual familiarity with technology.

'E-safety' will be taught to children starting as part of the PSHE curriculum in Years 3 and 4 and this curriculum will develop as the children move into the upper key stage 2. This will be done without the use of screens / computers in the lower key stage 2 classes, but will start to involve screens and computers as the children move to upper key stage 2.

This policy applies to all staff and children once they reach the appropriate age and are given access to the school internet system.

Young people will develop an understanding of the uses, importance and limitations of the internet

- Young people will be taught how to effectively use the internet for research purposes.

- Young people will be taught to evaluate information on the internet.
- Young people will be taught how to report inappropriate web content.
- Young people will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Young people will use the internet to enhance their learning experience.
- Importance of understanding the addictive nature of technology and its impact on attention spans and health.
- Young people have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

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.

Links with other Policies

Many of the risks connected with computers reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. The schools Behaviour Management Policy, The Anti-bullying Policy and the schools Safeguarding and Child Protection Policy). Any incidents of cyberbullying or other e-safety incidents listed in this policy which occur outside of school will also be dealt with in school in line with the policies listed above. Parent/carers will be informed of such behaviour even if it is out of school.

Advice for parents

The school asks that parents' guide their children in the appropriate uses of electronic media outside of the school environment. Parents would be welcome to speak to teachers about their questions and challenges related to media so that together they can work out viable approaches. Ensuring that the children have a rich, natural environment around them in their home life can help limit media use in conjunction with clear limits. For all children we recommend limited or no computer/screen access during the school week. We recommend that while the children attend Inwoods that they are given no personal devices such as smart phones or watches.

- Set ground rules. Discuss. Continue to talk.
- Limit the amount of time online and using screens.
- Use ISP filtering.
- Set up a family e-mail account for registering on websites, competitions etc.
- Monitor online activity (recently visited sites, click the History button).
- Software for filtering isn't fool proof - combine with supervision.

- Check temporary files (open Internet Explorer and select Internet Options, on the General tab under Temporary Internet Files, click the Settings button and then click View Files).
- Contact CEOP or the police if you suspect grooming.

CEOP (Child Exploitation & Online Protection) is dedicated to eradicating the sexual abuse of children, and is affiliated to the Serious Organised Crime Agency (SOCA). UKCIS (UK Council for internet safety) also have many useful resources.

Safer search engines:

- www.kiddle.co
- www.safesearchkids.com

Further information and advice:

- childnet.com (select 'Know It All' for a wide range of links to other sites)
- google.co.uk/goodtoknow (select 'Stay safe online')
- getsafeonline.org
- kidscape.org.uk

Useful information can also be found at: https://www.gov.uk/government/publications/preventingand-tackling-bullying

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

Firewall and protection software

The School uses firewall devices from Untangle (part of Arista Networks) to implement filtering and 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 Provider in conjunction with BrightCloud. 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 Team and the IT Administrator. They have consideration to 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 teacher will be working alongside the pupil using the computer
- Internet browsing history and web logs are maintained for the computer accessible to pupils and can be examined if the software raises an alert. The School uses Arista for monitoring. Arista Threat management Software 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 the children. The school computer has a fixed IP and activities on the computer are logged. The reports produced by Arista are sent to the DSL by the IT Administrator every two weeks or more frequently depending on the level of concern that are reported for further action.

Incidents and response

Where a child 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.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying 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 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.

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 Designated Safeguarding Lead will be informed of digital safety concerns, as appropriate. The Designated Safeguarding Liaison Trustees will report to the Board of Trustees on online safety practice and incidents, including outcomes, 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 the IT Administrator. 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.

Social Networking

It is to be recognised that staff are also likely to use social networking sites in their recreational time on their own personal computers. This form of activity is not to be discouraged; however, staff must agree and adhere to a 'professional conduct agreement'. It must be ensured that the use of such sites will not compromise professional integrity or bring the school into disrepute.

It must be recognised that social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyberbullying, for example, is to be considered as unacceptable as any other form of bullying and effective sanctions must be in place to deal with such concerns. Any known or suspected incidents must be reported immediately to the Designated Safeguarding Lead.

Staff must not have a pupil as a 'friend' or contact on any social networking medium.

Use of Cookies by the Krishnamurti Foundation Trust

On the school website to make this site work properly, they sometimes place small data files called cookies on the device you use. Most big websites do this too.

What are cookies?

A cookie is a small text file that a website saves on your computer or mobile device when you visit the site. It enables the website to remember your actions and preferences (such as login, language, font size and other display preferences) over a period of time, so you don't have to keep re-entering them whenever you come back to the site or browse from one page to another.

How do we use cookies?

We use two types of cookies on our website: per session cookies, which are temporary cookies that remain in the cookies file of your browser until you leave the site; and persistent cookies, which remain in the cookies file of your browser for longer (although how long will depend on the lifetime of the specific cookie). These cookies are used to store state information between visits to a site.

How to control cookies

You can control and/or delete cookies as you wish – for details, see aboutcookies.org. You can delete all cookies that are already on your computer and you can set most browsers to prevent them from being placed. If you do this, however, you may have to manually adjust some preferences every time you visit a site and some services and functionalities may not work.