ICT USE, Technology, e-SAFETY AND COOKIE POLICY

INWOODS SMALL SCHOOL

Last Review Date	September 2021
Policy endorsed by	The Trustees and Principal
Policy is maintained by	IT Administrator / Inwoods Coordinator
ISI reference	A6, B1, B9, A8, A9
Next review date	August 2022
Review body	School Coordinator and School Principal

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: Kate Power: Designated Safeguarding Lead (DSL) at Inwoods. If she is not available please contact Antonio Autor: Deputy Designated Safeguarding Lead (DDSL). If neither 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. Furthermore, at Inwoods, a healthy respect for nature and silence are nurtured, from which creativity, generosity and social conscience have the time to grow. The children best learn to use electronic media as a resource and tool when these media are introduced after children have developed a rich experiential foundation. Media thus becomes a supplement to, not a substitute for, the richness of direct experience.

With this in mind we provide no computer access / screens for younger children and limited access for Year 5 and Year 6 children, but there is consideration for the role of technology within our curriculum from Year 1 to Year 6.

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 - either privately or with other parents - 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.

Access to the Internet

At Inwoods Year 5 and 6 children are allowed limited internet access in school at the discretion of the teacher to help in studies. 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
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cybersquatting
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

When children are using computers, they are to be sited 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.

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. behaviour, anti-bullying and child protection policies). Any incidents of cyberbullying or other e-safety incidents listed in this policy which occur outside of school will still be dealt with in school in line with other policies such as the

behaviour policy, child protection policy, the anti-bullying policy. Parent/carers will be informed of such behaviour even if it is out of school.

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 camera. 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.
- Young people have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Advice for Young people

- Don't publish identifying information.
- Pick a username that doesn't include any personal information.

- Set up a separate email account that doesn't use your real name and use that to register and receive mail from any site. That way if you want to shut down your connection, you can simply stop using that mail account.
- Use a strong password (at least 8 characters; mixture of lowercase letters, uppercase letters, numbers and symbols).
- Keep passwords safe, and change them regularly.
- Keep your profile closed.
- Only allow friends to view your profile.
- What goes online stays online. Don't say anything or publish pictures that might cause you embarrassment later. If you wouldn't say it to your parents, don't say it online!
- Be on your guard.
- Talk to parents/carers if you feel uncomfortable.
- Save or print evidence.

Advice for parents

- 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:

- askkids.com
- yahookids.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

Control Measures

The following control measures will be put in place which will manage internet access and minimise risk:

- Secure broadband or wireless access.
- A secure, filtered, managed internet service provider and/ or learning platform.
- Secure email accounts.
- Regularly monitored and updated virus protection.
- A secure password system.
- An agreed list of assigned authorised users with controlled access.
- Clear Acceptable Use
- Effective audit, monitoring and review procedures.

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.

Cookies

To make this site work properly, we sometimes place small data files called cookies on your device. 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.