Newbury Hall
SCHOOL

E-SAFETY POLICY

Date	Review Date	Contact
01.03.19	01.03.20	Head of School & Education

This policy is underpinned by Newbury Hall's core values as stated in our aims & ethos.

This policy relates to all members of the Newbury Hall community (including students, staff, visitors and contractors) who have access to and are users of ICT systems and resources both in and out of learning contexts where actions relate to school activities or use of school online systems.

Internet-blocking technologies are continually updated and harmful sites are blocked by our filtering system. Newbury Hall's wifi, monitored by Instill Education Ltd, uses SonicWALL firewalls with the Comprehensive Gateway Security Suite. This provides website filtering for categories such as pornography, violence, hate and weapons. It also includes anti-virus and anti-malware protection.

The school wifi is limited to daytimes and evenings; it is turned off at night.

Aims

To prepare students for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve, exchange and use information via technology, and to provide a safe environment in which to do so.

Context

Computer skills are vital to access employment and lifelong learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings our staff and students into contact with a wide variety of influences, some of which may be undesirable.

These new technologies are enhancing communication and the sharing of information, which inevitably challenges the definitions and boundaries of the school environment. Current and emerging technologies used in school and, in many cases more importantly, outside the school by students include:

- Internet websites
- Instant messaging
- Social networking sites
- Emails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones, tablets and computers with e-mail and web applications

All of these have potential to help raise standards of teaching and learning, but may equally present challenges to both students and tutors in terms of keeping themselves safe. These challenges include:

- Exposure to inappropriate material
- Cyber-bullying via websites, social media, mobile phones or other technologies
- Identity theft or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising
- Online gambling
- Financial and other scams
- Safeguarding issues such as grooming (children or vulnerable adults)
- Other illegal activities

At Newbury Hall we seek to maximise the educational benefit that can be obtained by exploiting the use of ICT, whilst at the same time minimising any associated risks. By making clear to students, staff, visitors, contractors etc what the school expectations are regarding the use of ICT, we aim to protect our students and staff from harm as far as is reasonably practicable. The precise nature of the risks faced by users will change over time as technologies, fads and fashions change but there are general principles of behaviour and conduct that apply to all situations, for example:

- all users needing to know what to do if they come across inappropriate material
- staff not giving out personal information such as phone numbers or email addresses to students
- staff not allowing access to their social networking accounts, etc

We also communicate to students on our courses that they should not give out personal information such as telephone numbers, addresses etc to strangers or publish this information on social networking sites. This is done through PSHE lessons, throughout the curriculum generally, and through visiting speakers.

Roles and responsibilities

Staff

All teaching and non-teaching staff (including suppliers and contractors) are responsible for supporting safe behaviour throughout the school and following e-safety procedures. All school staff should be familiar with this E-safety Policy as well as the the Code of Conduct (Staff) and Safeguarding & Child Protection Policy.

- Participate in any e-safety training and awareness-raising sessions
- Act in accordance with this E-safety Policy
- Report any suspicion of misuse to the Designated Safeguarding Lead
- Refrain from making negative comments about the school or members of its community on any blogs or social networking sites. Negative comments such as these could be considered as gross misconduct as it potentially affects the reputation of the school and/or lowers morale
- Help educate students in keeping safe, especially vulnerable groups. Whilst regulation and technical solutions (such as filtering systems) are important, they must be balanced with educating students to take a responsible approach. The education of students in e-safety is an essential part of using technology in classes
- Act as a good role model in their own use of ICT.
- Where internet use is pre-planned in sessions or enrichment activities, students should be directed to sites which are appropriate for their use and procedures should be followed for reporting any unsuitable material that is found on internet searches. Where practicable staff should pre-check sites and any possible search results

- Where students are able to freely search the internet in school, staff should be vigilant in monitoring the content of websites in case there is any unsuitable material
- Be aware of the potential for cyber-bullying where malicious messages, for example through the use of forums and social networking sites, or via internal class emails or text messages on mobile phones etc, can cause hurt or distress
- Students should be taught to be critically aware of the content they can access online and be guided to validate the accuracy of information
- Students are educated as to the need to acknowledge the sources of any information used and to respect copyright when using material accessed on the internet
- Use the BCC address label when sending emails to groups of students

Students

Students are encouraged to access various technologies in lessons and in the completion of assignments and independent research, and are therefore expected to follow school policy. They should fully participate in e-safety activities and report any suspected misuse to a member of staff.

Students are expected to behave in a safe and responsible manner, treating equipment with respect and using school resources, including school wifi, only for educational purposes, positive social interaction or to contact parents, etc.

Students are expected not to:

- use email, social media or blogs etc to make negative comments, bully or insult others
- waste resources, including internet and printers
- have any inappropriate files, for example copyrighted or indecent material
- attempt to circumvent or hack any systems
- use inappropriate or unacceptable language online
- reveal their personal details or passwords
- visit websites that are offensive in any way
- use chat rooms or newsgroups
- do anything online or using ICT that could damage the reputation of the school
- download anything inappropriate or install any programs onto school devices.

The Senior Leadership Team

The Senior Leadership Team at Newbury Hall takes e-safety very seriously and aims to ensure that policies and procedures are in line with best practice and the safeguarding agenda. In particular, they aim to ensure that all staff receive suitable training to carry out their e-safety roles and sufficient resources are allocated to the task. Senior leaders will follow the correct procedure in the event of a serious e-safety allegation being made against a member of staff and implement the wider organisation's system for monitoring and improving e-safety. This includes making sure that the academic network infrastructure is safe and secure and that policies and procedures approved within this policy are implemented. Consideration of e-safety issues arising will inform the annual review this policy.

Responding to issues

It is important that any incidents are dealt with as soon as possible in a proportionate manner and that members of the school community are aware those incidents have been dealt with.

Any concerns around the misuse of ICT will follow the procedures described in the Safeguarding & Child Protection Policy where there is potential or real harm to another person; disciplinary procedures and the Behaviour Management Policy may also be invoked.

Where an allegation has been made against a student, an investigation will take place by the Designated Safeguarding Lead, Head of School & Education and/or other senior staff members. The outcome of the investigation will decide what the consequent appropriate course of action will be, and depending on the nature of the misuse the student could be suspended from classes until the investigation is complete. The sanction will depend on the seriousness of the misuse and whether it was accidental or deliberate, a first-time offence, thoughtless or malicious, etc. Sanctions could involve the student having ICT access removed for a period of time or, in very serious cases, suspension or exclusion. Where there is a potential legal issue the Head of School & Education together with designated persons will decide on the need for the involvement of outside agencies, including the police.

Signed:

Alex McNish, Head of School & Education, on 01.03.19