INDEPENDENT CHILDREN'S SCHOOL AND HOME
OWLSWICK

Owlswick School and Home
Acceptable Use of the Internet Policy

Approved by:	Leon Creenan	**Date:**	29/11/18
Last reviewed on:	29/11/18		
Next review due by:	29/11/19		

Introduction

Owlswick has provided computers/ICT systems for use by young people and the Care and Education Teams. They offer access to a vast amount of information for use in both studies and recreational activities, acting like an extension to a library and offering great potential to support the curriculum, learning and the building of knowledge. This policy applies to young people and staff alike.

The computers/ICT systems are provided and maintained for the benefit of all young people and staff, who are encouraged to use and enjoy these resources, and ensure they remain available to all. Young people are responsible for keeping themselves safe when using the Internet in a classroom or within the home. Access to computers for the young people is viewed as a privilege, not a right, and inappropriate use will result in that privilege being withdrawn.

Guidance for the use of Equipment

All young people and staff are not permitted to:

- Install, attempt to install or store programmes of any type on the computers/ICT systems without the express permission of senior managers
- Damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Use the computers for commercial purposes, e.g. buying or selling goods.
- Open files brought in on removable media (such as floppy disks, CDs, USB drives etc.) until they have been checked with antivirus software, and been found to be free of viruses.
- Connect mobile equipment to the network (e.g. laptops, tablet PCs, PDAs etc.) until they have been checked with antivirus software, and been found to be free of viruses.
- Eat or drink near computer equipment.

Guidance for Security and privacy

All young people and staff must not:

- Disclose their password to others, or use passwords intended for the use of others.
- Tell anyone they meet on the Internet their home address, telephone number, any details about Owlswick School and Home, or send them any pictures. Please see the Owlswick Safe use of the Internet and Social Media Policies for further guidance.
- Use the computers in a way that harasses, harms, offends or insults others.

- Disrespect, or attempt to bypass, security in place on the computers, or attempt to alter the settings.

Guidance for use of the Internet

Staff must ensure all young people abide by the following protocols:

- The Internet should only be used for study or for authorised/supervised recreational and leisure activities.
- The Internet is not used to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive or anything that could place themselves at risk.
- All young people respect the work and ownership rights of people outside the school, as well as other young people or staff. This includes abiding by copyright laws.
- Do not arrange to meet anyone via the Internet. Please see the Safe use of the Internet/Social Media Policies for further guidance.

Guidance for use of Email

Staff and young people must abide by the following protocols:

- Be polite and appreciate that other users might have different views from their own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone they already know and trust. They could contain viruses or other programs which could destroy information and software on the computers.
- The sending or receiving of emails containing material likely to be unsuitable for children or schools/homes is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff

Guidance for the use of Enforcement of the Policy

This document is to be read carefully by all staff. A copy will be made available to each staff member. If any staff member disregards or negates the policy, disciplinary action may be taken and where appropriate, the police informed, or other legal action taken.

For young people, an e-safety agreement is in place which all young people are expected to sign and adhere to. Additional action may be taken by Owlswick in line with existing policy regarding social media or internet use. For serious breaches of the policy further

action may be taken with the young person and this will be discussed with them as appropriate.

Acceptable use of Internet and email facilities for young people and staff rationale

Owlswick has a responsibility to transform and enhance young people's education and help individuals to fulfil their potential and raise standards with ICT. However, Owlswick also has a duty of care and must ensure the constant safeguarding of young people and staff. It is also important that young people learn how to be safe when they are using new technologies. Whilst blocking and banning specific internet sites is part of the Owlswick e-safety policy, staff will seek to equip young people with the skills and knowledge they need to use the Internet and Social Media safely and responsibly, managing the risks wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school and in the home and beyond.

Risks of using the Internet

The Byron Review (Safer Children in a Digital World 2008) classified the risks of using the internet as relating to content, contact and conduct. The risk is often determined by behaviours rather than the technology itself. These can include (and the list is not exhaustive):

- Commercial
- Aggressive
- Sexual
- Values
- Content (young person as recipient)
- Adverts, spam, sponsorship
- Personal Information
- Violent/hateful content
- Pornographic or unwelcome sexual content
- Bias, racist and/or misleading information/advice
- Contact (young person as participant)
- Tracking
- Harvesting personal information
- Being bullied, harassed or stalked
- Meeting strangers
- Being groomed
- Self-harm
- Unwelcome persuasions
- Conduct (young person as actor)
- Illegal downloading
- Hacking
- Gambling

- Financial scams
- Being radicalised
- Terrorism
- Sexual Exploitation
- Bullying or harassing one another
- Creating and uploading inappropriate material
- Providing misleading information/advice

Principles for acceptable use of the Internet

Staff will use the internet to investigate and research subjects, cirriculum themes or topics related to young people's social and personal development or recreational activities.

Online and other activities which are not permitted include:

- Searching, viewing or retrieving materials that are deemed inappropriate and/or break set guidance about accessing certain banned/blocked websites.
- Copying, saving or redistributing copyright-protected material, without approval.
- Subscribing to any services or ordering goods or services, unless specifically approved by Owlswick.
- Playing computer games or using other interactive 'chat' or 'social' sites unless specifically approved by Owlswick.
- Using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages).
- Publishing, sharing or distributing any personal information about a user (such as: home address; email address; phone number; etc).
- Downloading software.
- Taking and storing images of young people using mobile phones.
- Care staff are only permitted to use the Internet for personal use for limited periods during each shift.

Owlswick will:

- Use the Safe Search secure firewall to filter and monitor access. This secure system will provide reports on all internet use which will inform risk assessments for y/p and how and when the internet can be accessed.
- Ensure virus and anti-malware protection is installed and updated regularly.
- Regularly discuss acceptable use with young people and staff and remind them of Owlswick's policy and rules regarding e-safety.
- Educate and support parents/carers in the safe use of the Internet and other technologies.

- Ask parents to give consent for their young person to use the Internet.
- Ensure teaching staff guide pupils toward appropriate materials on the Intranet/Internet when in school.
- Appoint an e-safety champion for both School and Home . These champions will take the lead in ensuring the e-safety policies are adhered to as well constantly being updated. There is also a defined link between these champions and the designated child safeguarding leads for home and school.
- Ensure only those people with authorised access can access the school's IT network.
- Guest logons are to be given to supply teachers and other occasional staff where necessary.

Young people will:

- Have equal access to a variety of approved websites via the Internet.
- Be taught all the skills in order to use Internet and email as an ICT tool.
- Know how to report any concerns they may have.
- Use Internet and email to support, enhance and develop all aspects of their knowledge and learning.
- Develop Internet and email skills at the appropriate level regardless of race, gender, intellect and emotional or physical difficulties.
- Receive E-Safety training during every academic year.

Staff will:

- Ensure they keep data safe and secure.
- Conduct themselves professionally online; they must not allow young people access to their own data through social networking sites such as Facebook; staff will block young people who attempt to contact them.
- Inform the e-safety champions or senior managers of any issues of concern.

Useful Reference Websites

- www.teachernet.gov.uk
- www.thinkuknow.co.uk/teachers
- www.childnet.com
- www.kidsmart.org.uk
- www.ceop.gov.uk/reportabuse/index.asp
- www.everychildmatters.gov.uk
- www.nen.gov.uk/hot_topic

Monitoring, evaluation and review

Monitoring and evaluation are essential to any effective policy and provide essential feedback for the development of policy and procedures. For this reason, Owlswick will periodically ask staff and young people how this policy is performing and how it can be altered to help and protect all users. To be reviewed on a regular basis with a formal review once a year.