INDEPENDENT CHILDREN'S SCHOOL AND HOME
OWLSWICK

Owlswick School and Home

Internet Safety Policy

Approved by:	Sarah Hawke	**Date:**	24/11/18
Last reviewed on:	24/11/18		
Next review due by:	24/11/19		

INDEPENDENT CHILDREN'S SCHOOL AND HOME
OWLSWICK

Owlswick School and Home Internet Safety policy

Owlswick is committed to keeping the young people in our care and education setting and our members of staff as safe as possible when accessing technology and this policy provides guidance for the safe use of all devices, Internet and social media, regardless of where and how these are accessed.

Technology and the internet is an integral part of everyone's life. Young people at Owlswick need to learn how to use technology and the internet safely and effectively as well as understanding their personal responsibility in this fast-changing and developing area.

Owlswick's aim is for young people to use all forms of technology safely and the emphasis for young people and staff is education and developing self-confidence and awareness when using electronic devices and social media. We aim for young people to act as an appropriate citizen when using technology and in return expect to be treated appropriately by others.

Young people can access modern technology, social media sites and the Internet in many different ways, using a variety of devices, including desk top computers, lap tops, mobile phones and games consoles.

Our key messages for young people when using technology or the internet are:

- Educate
- Empower
- Prevent
- Protect

Our aim is to keep an open dialogue with young people about internet safety and E-safety and have conversations about the risks whilst promoting how the internet and technology can expand knowledge and be enjoyable to use. We want young people to understand that their digital footprint will follow them wherever they go in their lifetime and that there can be consequences for their futures in terms of employers vetting their histories or risks to their personal safety if they become involved with someone they do not know.

Owlswick treats internet safety as a safeguarding and child protection issue not an ICT issue. It covers the use of all technology and is not limited to the equipment used by young people and staff members. Internet safety is the responsibility of everyone at Owlswick and all staff and young people have a role to play in keeping everyone safe whilst enjoying and learning from the Internet and all other forms of electronic communication. All staff have a duty to be aware of internet at all times. It is not limited to school or home premises, equipment or just involves the school day. Staff provide an emphasis on young people being taught safe

practices and the staff internet safety champions, Designated Child Protection Lead and Management Team will ensure that this policy will be monitored and enforced.

Related Policies

This policy should be read in conjunction with the following Owlswick policies and procedures:

- Owlswick School and Home Staff Handbook
- Owlswick School and Home Child Protection and Safeguarding Policy and Procedures
- Owlswick School and Home Social Media policies
- Owlswick School and Home Anti-Bullying Policy
- Owlswick School and Home Missing Person's Policy
- Owlswick School and Home Tackling Extremism and Radicalisation Policy

The Internet

Owlswick cannot make the internet completely safe but can put in place safeguards to minimise the risk of young people coming to harm (when they are accessing web sites for example). Owlswick also has a responsibility to ensure that young people are confident in using the Internet and understand the action they can take if they inadvertently view material that is unsafe or inappropriate.

This includes building knowledge and understanding of social networking sites and the potential risks of interacting with strangers or understanding how a person can be the victim of cyber bullying for example.

Safeguarding and Child Protection

Owlswick is committed to ensuring that young people are safeguarded in all aspects of their lives and that individuals can expect to feel safe and be kept safe in their home and school environment.

Safeguarding and child protection covers and is related to a number of areas which relate to the risks of young people being for example:

- Sexually exploited and a victim of child sexual exploitation
- Becoming radicalised or involved in acts of extremism
- Going missing
- Becoming involved in gang culture or crime
- Becoming the victims of crime
- Being bullied

All of the above areas can be related to internet safety as the internet and social media are used to groom and exploit young people after gaining their confidence and adults or other young people seeking to form relationships.

All young people have a linked key worker from the care team who will be responsible for completing an internet safety agreement with them for the use of all technological devices within the house. Each young person also completes an internet agreement for using computer equipment and software programmes in school.

If an internet safety incident occurs regarding a young person, staff will follow a set procedures and report this incident (using the internet incident reporting process) to the Designated Child Protection Lead (DCPL). The DCPL who will make a decision about the immediate action needing to be taken and if the child protection policy needs to be evoked. In the absence of the DCPL, the incident would be reported to the senior manager from home or school for a decision about the action to be taken.

There are strict guidelines set out in the Owlswick internet safety policy regarding how staff monitor the use of the internet and social media by young people in order to ensure they are being safeguarded. Please refer to Internet Safety Social Media policy.

Owlswick's primary aim is to educate young people to feel and be safe when using the internet and social media as well as to enjoy exploring and being able to be creative. However there is a safeguarding requirement to ensure that certain sites are not available to individuals or groups if they search on-line or try to connect to a certain site which may show pornographic images for example.

All the safeguarding and monitoring procedures and systems have a reference to the national requirements and regulations on Children's Homes to safeguard young people.

It is the role of all staff to ensure that all policies related to internet safety are being adhered to, support the internet safety education agenda for young people, encourage the young people to learn how to use technology safely and to ensure that national directives and monitoring requirements are being met and, where possible, surpassed.

Further measures taken by Owlswick to keep young people safe and monitor their use of electronic devices/Internet and social media use are as follows:

- The school and young people's network is fitted with a software programme which enables certain websites and subject areas to be blocked and then cannot be accessed (e.g. sites which show violent or pornographic images). This programme is regularly reviewed and new sites are added to be blocked where necessary.
- Privacy settings and parental controls are set on all communal computers and a time lock is set on all computers meaning they can only be used within certain times. Young people can also only access Internet programmes and/or games which are age appropriate and in line with national guidelines.
- All school computers and lap tops are password protected which can only be unlocked by a member of staff

All young people have passwords for their own accounts in the home and are encouraged to change these regularly and not share them with anyone else. They are aware they need to log off after they have used a computer and not leave their accounts running.

Within the school environment personal passwords are set but not shared with the young people. Teaching staff take responsibility for logging students on and off school devices. They are aware they need to log off after they have used a computer and not leave their accounts running.

If there is a concern that a young person has been accessing internet sites which are not appropriate or an issue has been flagged via a social media site then staff may check the history of a mobile phone or personal lap top. Young people are aware that staff may take this action and the reason why. This action will not be taken unless the young person has been warned that this check may take place and will be made with them present. Monthly checks on all y/p personal devices will also take place. All checks made will be recorded as having taken place.

Owlswick requires young people who have a Facebook account to be a friend of Owlswick's own Facebook page and this page is constantly monitored to look at posts made and pictures added. Young people will also not be allowed to open a Facebook account unless they are of the required legal age.

Owlswick aims to educate young people in both home and school about using technology safely and securely and encourage the reporting of any issues or incidents of concern to staff so that immediate action can be taken. Part of this education is regarding the personal responsibility agenda for each individual young people and the measures they need to take to keep themselves safe.

Staff receive training in internet-safety and how to keep young people safe when using technology and are responsible for ensuring that their working practice keeps pace with this ever evolving area of safeguarding

Owlswick internet safety systems

Owlswick has invested in a new software security system called Safe Search which is enabled by a specialist external Internet safety company Connect Digital.

CONNECT
DIGITAL SECURITY

Connect Digital Security provide Owlswick with a fully managed and monitored security gateway solution, essentially which is a next generation firewall. This device has been configured to decrypt any SSL encrypted websites (with exception of banking sites) to ensure full inspection of all traffic can be performed and controlled.

- SSL Decryption
- Threat blocking using Intrusion Prevention System (IPS)

- Web filtering to block the following web categories:
    - Sexually Explicit images
    - Nudity and nude images
    - Anonymizers
    - Controlled substances
    - Legal highs
    - Hunting & Fishing
    - Intellectual Piracy
    - Cannabis and drug paraphernalia
    - Criminal Activity
    - Pro-Suicide & Self harm
    - Gambling
    - Militancy & Extremist
    - Phishing & Fraud
    - Extreme
    - Weapons

- Application Filtering to block high risk applications
- Malware prevention using gateway AntiVirus
- Search Engine Safe search enforcement
- Time enforced internet access

This system also enables Internet sites/programmes to be blocked by the moderators of the system who are senior managers. It also will prevent young people from being able to view certain images and sites that are embedded in Youtube videos for example. Senior managers will receive an immediate report which provides data on the sites that have been accessed by an individual young people, indicates which blocked sites have attempted to be accessed, which websites have been most visited, games and apps visited and how long has been spent on the internet. These reports are then acted upon if they raise any issues of concern about personal safety as well as inappropriate searches, illegal material or viewing/contact activity.

The IT routers have been set to Google Safe Search which does not allow any embedded pictures or thumbnails in websites searched or accessed to appear as these are often inappropriate or may compromise personal safety in some way.

An additional safety system has been installed by managers which can enable access to individual I.P addresses on lap tops and mobile phones. This means that devices can be blocked if they are being used to access websites or chatrooms for example that are not appropriate for the young person to view or participate in. Staff will have a conversation with the young person about what they are accessing and risk assess this in order to agree if a website can be further accessed for example. This is part of educating the young people about how to use the internet safely.

Staff will ensure that each personal lap top/tablet is set with parental controls/anti-virus software if a young person wishes to use this whilst at Owlswick. Staff will also have conversations with parents/carers and give advice about parental controls and safety measures as needed.

Each young person needs to add Owlswick as a friend onto their personal face book page if they wish to use Facebook at Owlswick. No young person is able to set up a Facebook account at Owlswick unless they are aged 13 or over. This is the case for other social networks and staff will monitor the social media sites being accessed. Young people are also advised to turn off location services on personal devices.

Managing and Reporting e-safety incidents
Owlswick has an internet safety flowchart which guides staff and young people on the process to follow and action to be taken when an incident occurs.

If an internet safety incident occurs regarding a young person, staff will follow the set procedure and report this incident (using the internet safety incident reporting process) to the Designated Child Protection Lead (DCPL) who is the Registered Manager or the Deputy DCPL (Deputy Home Manager) or DCPL of the School (Head Teacher).

The DCPL or other lead will make a decision about the immediate action needed to be taken and if the child protection policy needs to be evoked. The internet safety incident reporting process will be followed and ensure the appropriate action is taken and the incident dealt with promptly with an emphasis on safeguarding the young person throughout the process.

Young people are encouraged to report anything they feel unsafe or concerned about to any member of staff and this will then be acted upon.

The Physical ICT Environment and Data Management/Transfer

Owlswick has built a specific IT network for the young people to access when they are in the home environment. This network is set to be accessed within agreed times and has the Connect Digital security and monitoring system applied which is used to block websites and domains which are deemed to be not appropriate or unsafe for the young people to access. This network is regularly monitored and amendments made with the aim of constantly improving the safeguarding of young people.

There is an enforced password change policy in place for all staff and they are prompted to change their policy every 90 days, using an alpha/numeric password. Staff will also not log on using any other username/password other than their own.

All office lap tops will only be used by Owlswick employees and are to be securely locked away when not in use. School ICT equipment will only be used by young people under the supervision of staff. Any young person with a Local Authority issued lap top will have anti-virus and monitoring software already installed which is monitored by both the Local Authority and Owlswick staff.

All Owlswick's access points run on WPA2 encryption and are compliant in this area.

No data regarding any young person/staff member should be transferred off site using an electronic or other method. Any data that needs to be accessed away from Owlswick such as operational policies for example will be moved using approved USB memory encryption keys that have been issued by Owlswick. No personal USB sticks are to be used by any member of staff to transfer or store data.

Any data that is to be moved off site via a lap top or encrypted USB stick for example needs to be approved and checked by the Registered Manager for the care staff and Head Teacher for the education staff and must be for a specific reason. Staff must not transfer information from an offsite internet site for example onto an encrypted USB stick that will then be used at Owlswick due to the risk of virus/spy ware or malware transfers onto the Owlswick network. Staff must also ensure that it is their responsibility to ensure any material contained in files is fit for purpose and does not contain any offensive or copyright material.

All personal records for staff are kept locked in secure filing cabinets. All personal information regarding young people is kept locked within the office environments. All child protection records are kept locked in a secure filing cabinet.

Use of ICT and ICT equipment in school

Guidance for Education Staff

- All use of school ICT equipment must be supervised by the members of the education team at all times when the equipment is being used during the school day.
- No piece of equipment should be accessed by a young person in a private space within the school building.
- All school ICT equipment will be password protected and these passwords will be accessible to staff only.
- No young person will use the ICT equipment if they are alone in a classroom.
- No school ICT equipment will be accessed outside of the school day unless the Head of School has given their express permission for the equipment to be used. If this permission has been given then the use of this equipment by a young person will be fully supervised by staff.
- When using software for ICT lessons all programmes need to be checked and approved by the Head of School and lead for ICT before these are accessed by the young people.
- Parental controls have been set up for the use of the Internet meaning that if certain words or phrases are typed into a search engine then these sites will be automatically blocked. These controls are reviewed and adjusted on a regular basis by the Head of School and lead for ICT.
- The vision of the school is to educate each pupil in order for them to feel safe whilst using and enjoying the Internet but also to understand and cope with the issues that accessing certain web sites may bring (e.g. cyber bullying) and any concerns about their personal safety and well-being.

- All pupils are encouraged to report any suspicious sites to staff and adopt a 'think before you click policy' as detailed in this policy.
- Staff must ensure that the privacy settings are set appropriately for each computer and account holder when websites are being accessed.
- Staff must monitor that young people are not giving out personally identifiable information when using the Internet.

Use of ICT and ICT equipment in the home

Guidance for Care Staff

- All use of home ICT equipment must be supervised by the members of the care team. No piece of Owlswick ICT equipment should be accessed by a young person in a private space within the home building.
- Young people's personal ICT devices will be subject to a regular checks by care staff members in order to ensure that only age appropriate material and ICT content is being accessed. Controls are set as detailed above.
- The young people's internet server is set to be accessed at specific timed hours in order that inappropriate content cannot be accessed during the time when staff are unable to supervise the use of personal ICT equipment.
- All programmes need to be checked and approved by care staff members and lead for ICT when using software for uploading onto the ICT equipment.
- Parental controls have been set up for the use of the Internet. This means that if certain words or phrases are typed into a search engine then these sites will be automatically blocked. These controls are reviewed and adjusted on a regular basis by the home managers and lead for ICT.
- The vision of the home is to educate each young person in order for them to feel safe whilst using and enjoying the internet but also to understand and cope with the issues that accessing certain web sites may bring (e.g. cyber bullying) and any concerns about their personal safety and well-being.
- All young people are encouraged to report any suspicious sites to staff and adopt a 'think before you click policy' as detailed in this policy.
- Staff must ensure that the privacy settings are set appropriately for each computer and account holder when websites are being accessed.
- Staff must monitor that young people are not giving out personally identifiable information when using the Internet.

'Think before you click' – guidance for young people

Each young person is encouraged to use the following guidance in order for them to 'think before they click' onto a website/gaming programme:

- How do I know about this site/programme?
- Is the information likely to be right or could it have been altered by someone else?
- If there are other people on this site/programme how can I be sure that they are who they say they are?
- What information should I not give out about myself on this site?
- What do I do if I read or see something that makes me feel afraid, uncomfortable or unsafe? Who should I tell and when should I do so?

INDEPENDENT CHILDREN'S SCHOOL AND HOME

OWLSWICK

Established 1981 Registered and approved by the Secretary of State for Education.

OWLSWICK NEWHAVEN ROAD,KINGSTON, LEWES, EAST SUSSEX BN7 3NF **T:** 01273 473078 **E:** OFFICE@OWLSWICKSCHOOL.CO.UK
WWW.OWLSWICKSCHOOL.CO.UK

Delivering internet safety through the curriculum

Internet safety, and learning about what this means in practice, is part of the ICT lessons delivered within the classroom, as well as being built into other aspects of the curriculum (such as in citizenship lessons, for example). The awareness programme at the time of writing the policy is still to be fully developed. This will include areas such as cyber bullying and online grooming, using approved education tools such as video clips and discussion groups. The aim is to enable young people to explore these issues and show young people that they can be empowered to deal with them if needed.

The Internet is an essential tool in enabling young people to explore, research and experience new ideas or images as well accessing games and learning tools. The Internet within the school is not used without the young people being supervised by a member of the education team and web sites are constantly monitored to ensure age appropriateness relevant to the learning and exploring process. Lessons using the Internet are planned in advance and the education team constantly research the sites to be used.

Lap tops/Tablets/Personal Devices

Most young people have a personal lap top that has been given to them via their Local Authority. These lap tops are not able to access the Internet within the boundaries of Owlswick unless they have been given access to the Owlswick young person's network by a member of staff using a password protected process. If this permission is given the young person will use the lap top in the presence of a member of staff. All software on the lap tops have been placed there via the Local Authorities and checked by Owlswick staff in terms of parental controls.
Local Authorities have set their own parental controls for the lap tops which use a security software programme. Laptop devices provided by Local Authorities Education departments must remain in school at all times.

Owlswick will receive a next day report if a young person has tried to access inappropriate material or a blocked website. Staff will carry out spot checks on lap-tops/tablets/personal devices in order to ensure that any material stored is age appropriate. They may also do this if there are concerns about the sites or social media being accessed by a young person.

No member of staff will take a lap top/personal device belonging to Owlswick away from the school or home to work at home. There is a strict policy on data storage and removal and no data about any young person can be taken off site from the Owlswick premises. This is in line with the data-protection, records management and confidentiality policies. Staff will only use encrypted memory sticks for data storage and will only transfer documentation to be worked on outside of the Owlswick site that has been agreed in advance by their line manager.

Social networking

The young people at Owlswick are able to access social networking sites as long as they are of the age to become members of these sites. Parental controls have been set up by staff in order to monitor all postings on these type of networks whilst the young person are on the grounds of Owlswick in order to ensure that they are not putting themselves in an unsafe position.

It is important that all young people are able to learn to use social networks as safely as possible and enjoy being able to communicate with their peers using this form of communication. Staff need to actively support the use of the networks as long as the young people are following safe practice guidelines. There are strict guidelines in place about not identifying where the young person lives or any contact information about them.

Individual circumstances are assessed and certain invitations to family members, friends or carers are sanctioned if these relationships have had a detrimental effect on the health, safety and well-being of the young person in the past or present. These circumstances are reviewed on a regular basis in order to ensure that contact is not restricted if all involved in the care of the young person agree that contact with a family member for example has been assessed as been safe and appropriate to reinstate.

Young people will also be made aware of the legalities regarding activities such as sexting and 'revenge porn'. They will be informed and reminded that any images showing a young person under the age of 18 in an erotic or topless pose regardless of whether there is no sexual content is illegal and classified as 'an indecent image of a child'. They will be made aware that they may face criminal charges if they take part in any activity of this sort and will be reported to the Police.

Please refer to the Social Media Policies for further information.

Cyber bullying

Cyber bullying is a growing issue of concern for young people and Owlswick needs to ensure that young people placed with us are aware of this issue. By using the internet policy guidance and agreed control mechanisms, staff aim to educate and ensure awareness amongst the young people about cyber bullying. This education includes what the policy means in practice, what to do if they think someone is bullying them or what to do if they are in a conversation or communication which is making them feel uncomfortable, angry or upset. Young people need to understand the potential consequences of putting personal information about themselves online and that this information then becomes public property as they lose control of anything posted. They need to understand how this information may be used by person/persons unknown to them to manipulate them into contacting them, encouraging them into private conversations or arranging to meet them without the young person knowing their real identity.

Young people are encouraged to recognise and report cyber bullying if they think this is happening to them. Staff will then take the appropriate action and offer the necessary support to the young person to bring an end to the problem. Staff will also report any cyber bullying to the relevant agencies.

Please refer to the Anti-Bullying Policy for further information.

Online grooming/sexual exploitation

Online grooming is a particular issue of concern for Owlswick as many young people are vulnerable and some could possibly become a target for online grooming. By using the guidance and agreed control mechanisms, staff aim to educate and ensure awareness amongst young people about online grooming and what this means in practice. This includes the signs to look out for when one person is trying to 'groom' another.

Staff will also talk to the young person about what to do if they think someone is grooming them and if they have any fears or concerns about any conversations that they may be having online. This includes the continual raising of awareness of the fact that people may not be who they say are and being careful about the amount of personal information given out by the young people.

Please see the child protection and safeguarding policy for further information.

Young people going missing

Young people going missing is an issue which can be related to e-safety as individuals can enter into friendships or relationships with other young people or adults online who then encourage them to make a date to meet or leave their home without informing anyone. Staff will risk assess each young person and this will include if there is an identified risk of a young person going missing. Following the assessment they will then put in place preventative measures in order to mitigate this risk. This will include monitoring and may deemed necessary temporarily removing access to social media and the internet. This would only be undertaken in conjunction and with the agreement of parents/ carers and external agencies involved in the young person's care. If a young person continually goes missing then a case conference involving parents/carers and all external agencies will be arranged and an assessment of the placement undertaken which will consider if the young person can be kept safe.

Please see the missing persons policy for further information.

Sexting

Sexting is a word created two years ago and describes the use of technology to share personal and sexual content. It is a word-mix of sex and texting. Other nicknames young people may hear might be 'cyber sexing', 'doxing' or 'selfie'.

The content can be anything from sexual texts to partial nudity to sexual images and video. Very often it is between partners but can be between groups and uses a whole

range of devices, technologies and online spaces. However the most common ones are mobile phones, MMS, Skype, Facetime and social network sites where images can be posted and shared on Facebook, Twitter, Tumblr, Flickr, YouTube etc.

Young people need to be made aware that most sexting is deliberate, the person sending the content means it to happen. They will pose or act in a sexual way and will make direct effort to send it to the person they want to see it (usually a boyfriend or girlfriend). Accidental sexting is more likely to happen if their judgement is clouded, for example if they have taken alcohol or drugs or are under pressure from those around them. In these cases, the young person may become confused and randomly send the photograph, feel more sexually confident and less inhibited and less aware of risk and the consequences.

Young people need to be aware of whether they can trust the person to whom the message was sent. They also need to be aware that posting directly onto a social network makes it harder to regain the control. Networks and software devices such as Facebook, Twitter, YouTube, What's App, Instagram make it harder to regain that control; it is hard to know where images uploaded to these sites have gone or been stored. It is important for young people to understand the different ways in which they can contact and report to social network sites to request the removal of content. It is not enough to say 'I don't like it'. The request needs to show that it breaks the sites terms and condition. Staff will support young people in educating them about the risks of sexting and the consequences of putting an image online, and of then losing control of that image. They will also ensure that reports are made to the appropriate agencies as and when required. It is equally important that a young person understands that any image placed on any Internet site will never completely disappear.

Radicalisation/Acts of Extremism

Owlswick is aware that social media and the internet are used by certain groups to groom and recruit vulnerable people and there is a risk of an individual becoming radicalised and/or involved in an act of extremism.

All staff are trained have received PREVENT training which advises on how to monitor young people and assess the risks of them becoming involved with groups or individuals who may have an agenda which could make a young person unsafe. Staff will make a Channel referral to Sussex Police if required.

Young people also receive education and guidance regarding what being radicalised means and how they need to report this if they have concerns about anyone or group they have been in contact with. Staff will also monitor the websites being visited by young people and are vigilant to any signs that a young person may be exhibiting which can be related to radicalisation or extremism.

Educational Resources

Owlswick is a member of the Child Exploration and Online Protection Centre (CEOP) and is able to access educational tools and resources which can be used to educate and inform the young people in our care and education settings. This includes the

'Thinkuknow' website which includes a facility for young people to report online abuse. The programme of safety training and awareness-raising for both staff and young people are currently being revised and are there for all to access.

Owlswick has a relationship with the East Sussex County Council Schools ICT training consultants who provide regular training, advice and guidance to both Home and School about working practice, safeguarding and security measures.

Staff will also access resources from:

www.childnet.com
First to a Million
Kids.getwise.org
ChildLine zippit app