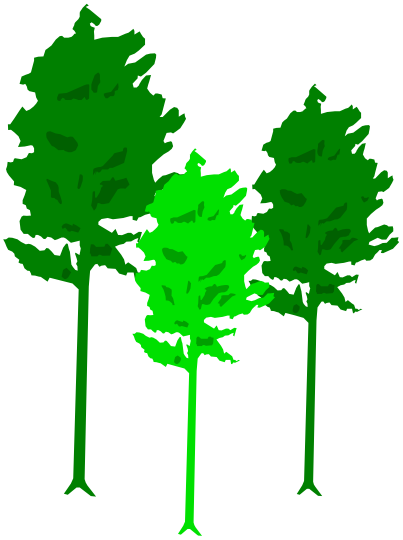
Online Safety Policy



WOODLAWN PRIMARY SCHOOL

June 2017

Principal: Mr I Mullen
School ICT Coordinator: Mr Proctor
Designated Teacher for Child Protection: Mrs M Beattie
Deputy Designated Teachers for Child Protection: Mrs K Edwards

Woodlawn Primary School
Online Safety Policy

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circulars 2011/22, 2013/25 and 2016/27 on e-Safety. This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Woodlawn Primary School. It also links to Article 17 from the UN Convention on the Rights of the Child which states:

"You have the right to get information that is important to your well-being, from radio, newspaper, books, computers and other sources. Adults should make sure the information you are getting is not harmful, and help you find and understand the information you need."

Internet access in school

Providing access to the internet in school will raise educational standards and support the professional work of staff.

Teachers and pupils will have access to web sites worldwide (including museums and art galleries) offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with people world-wide.

In addition, staff will have the opportunity to access educational materials and good curriculum practice, to communicate with the local education board, support services, professional associations and colleagues; exchange curriculum and administration data with the Department of Education and receive up to date information about issues that are relevant to school and learning.

In the longer term the internet may also be used to enhance the school's management information system and provide access to a school website to promote the work and achievements of the children and staff.

Parents' attention will be drawn to the policy by letter. Our school internet access policy will be available for parents and others to read on demand and on the school website.

This Online Safety policy operates in conjunction with other school policies including Positive Behaviour, Child Protection/Safeguarding Children, Anti-Bullying, Mobile Phones and other Related Technologies. Online Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the Northern Ireland curriculum and schools must ensure acquisition and development by pupils of these skills. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety in Woodlawn Primary School depends on effective practice at a number of levels:

- responsible ICT use by all staff and students; encouraged by education and made explicit through published policies;
- sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use;
- safe and secure internet provision by C2K and Classnet (provided by iTeach).

<u>Ensuring internet access is appropriate and safe</u>

The internet is a communications medium and is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection to the selection by publisher and teacher and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our internet access is provided by C2K and Class net (iTeach) which provides a service designed for pupils including a 'firewall' filtering system intended to prevent access to material inappropriate for children.
- Children using the internet will normally be working in the classroom, during lesson time and will be supervised by an adult at all times
- Staff will check that the sites pre-selected for pupils use are appropriate to the age and maturity of pupils

- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan
- Pupils will be taught to use the internet responsibly in order to reduce the risk to themselves and others
- The ICT co-ordinator will monitor the effectiveness of internet access strategies
- The ICT co-ordinator will ensure that random checks are made on internet history files to monitor compliance with the school's internet access policy
- The whole staff will ensure that the policy is implemented effectively
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed with advice from C2K and DENI

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature or information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. *Neither the school or C2K or DENI can accept liability for the material accessed, or any consequences thereof.*

A most important element of our rules for responsible internet use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly and at a number of levels. Responsibility for handling incidents involving children will be taken by the ICT co-ordinator and the designated child protection teacher in consultation with the pupil's class teacher. All the teaching staff will be made aware of the incident at the next staff meeting.

If one or more pupils view inappropriate material our first priority will be to give them support. The pupil's parents or carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents or carers and pupils to resolve any issue.

If staff or pupils discover unsuitable sites the ICT co-ordinator will be informed. The ICT co-ordinator will report the URL and content to C2K.

If it is thought that the material is illegal, after consultation with C2K, the site will be referred to the Internet Watch Foundation and the policy.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the rules for responsible internet use which have been designed to help protect them from exposure to internet sites carrying offensive material. If pupils abuse the privileges of access to the internet by failing to follow the rules they have been taught or failing to follow an agreed search plan when given the privilege of undertaking their own internet search, then sanctions consistent with our school behavioural policy will be applied. This may involve informing the parents or carers. Teachers may also consider whether access to the internet may be denied for a period.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images (illegal - The Protection of Children Act 1978); grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003);
- possession of pornographic images (illegal – Criminal Justice and Immigration Act 2008 criminally racist material in UK – to stir up religious hatred or hatred on the grounds of sexual orientation) (Illegal – Public Order Act 1986);
- promotion of any kind of discrimination;
- promotion of racial or religious hatred;
- threatening behaviour, including promotion of physical violence or mental harm;
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Additionally the following activities are also considered unacceptable on school ICT equipment provided by the school:
- using school systems to run a private business;

- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by C2K and/or Classnet;

- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;

- revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords);

- creating or propagating computer viruses or other harmful files;

- on-line gambling and non-educational gaming;

- use of personal social networking sites/profiles for non-educational purposes.

Cyber Bullying

Staff should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. Pupils engaging in cyber bullying may be dealt with in line with the school's 'Positive Behaviour Policy' and 'Anti-Bullying Policy'.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content;
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity;
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile;
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites;
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people;

Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour: It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

A record is kept of all incidents of cyber-bullying in the school's e-Safety log. This allows the schools e-Safety team to monitor the effectiveness of the school's preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

The E- Safety Team

- Mr I Mullen Principal
- Mr A Proctor ICT co-ordinator and C2k Manager
- Mrs M Beattie Designated Teacher for Child Protection
- Mrs K Edwards Deputy Designated Teacher for Child Protection

Maintaining the security of the school ICT network

We are aware that connection to the internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

The ICT co-ordinator will keep up to date with ICT news developments and work with C2K to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

School Ipads can access Wi-Fi through iTeach Wi-Fi called Classnet. This wifi and infrastructure has been installed and is maintained with an active, monitored filter system to satisfy both the needs of child protection/inappropriate content whilst ensuring that it serves to support teaching and learning.

This system exists in parallel to all C2K infrastructure. In line with DENI requirements the school has ensured that this additional service is:

a) filtered to standardised child protection levels; b) supported by trained staff in its use.

Access to the Classnet network is governed by unique device registration and pre-approval by authorised staff only (ICT co-ordinator and Principal). No devices can join the network without this approval and authentication.

Using the internet to enhance learning

Pupils will learn how to use a web browser. Older pupils will be taught to use suitable web search engines. Staff and pupils will begin to use the internet to find and evaluate information.

As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed and the age of pupils:

- Access to the internet may be by teacher demonstration
- Pupils my access teacher-prepared materials rather that the open internet
- Pupils may be given a suitable web page or a single web site to access
- Pupils may be provided with lists of relevant and suitable web sites which they may access
- Older more experienced pupils may be allowed to undertake their own internet search having agreed a search plan with their teacher; pupils will be expected to observe the rules for responsible internet use and will be informed that checks can and will be made on the files and the sites they access

Using information from the internet

We believe that, in order to use information from the internet effectively, it is important for pupils to develop an understanding of the

nature of the internet and the information available on it. In particular, they should know that, unlike the school library, most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited or edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on V
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true and understand that this is even more important when considering information from the internet
- When copying materials from the web, pupils will be taught to observe copyright
- Pupils will be made aware that the author of a web site or an email may not be the person claimed.
- Older pupils aware of safety when receiving and sending emails.

Internet access and home / school links

Parents will be informed that pupils are provided with supervised internet access as part of their lessons. We will keep parents in touch with future ICT developments by letter.

Internet use in pupils' homes is rapidly increasing and some parents may be grateful for any advice and guidance that school can offer – especially with regard to safe access for children.

- School guidelines on issues such as safe internet use will be made available to parents with printed information and internet sites providing information for parents about safe access for children
- The ICT co-ordinator will retain any relevant memos or emails regarding internet safety
- Internet Safety Day
- Websites-www.thinkuknow.co.uk and CEOP
- School website

School Website and School Social Networking

Woodlawn Primary School's website and Facebook page promotes and provides up-to-date information about the school and showcases other

aspects of school life. In order to minimise risks of any images of pupils on the school website or Facebook page being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions;
- Only photographs of children with parental/carer consent will appear on the school's website.
- No names will be included with photographs on the website.
- The website does not include home addresses, telephone numbers, personal e-mail or any other personal information about pupils or staff.
- The point of contact to the school i.e. school telephone number, school address and email address.

Mobile Phones and Other Related Technologies.

It is important to be aware of the safety issues regarding mobile phones and other devices which now increasingly have Internet access. For this reason, Woodlawn Primary School has a specific policy on the acceptable use of mobile phones and related technologies.

No mobile phones or other related technologies are brought into school by pupils, it is our policy that they should be confiscated while pupils are on the school's premises. If a mobile phone is switched on and used inappropriately, for example, cyber bullying, sending inappropriate text or images, the school's 'Positive Behaviour Policy' and if appropriate, 'Child Protection/Safeguarding Children Policy' 'will be adhered to.

Staff members should refrain from using their mobile phones or similar technology when in contact with children unless prior permission has been given by the Principal.

If photographs of pupils are being used by staff for lessons, presentations, website design etc., then they should be stored as much as possible on C2K system. If however, staff are working on school related activities on personal computers, any photographs stored should be kept to a minimum and transferred to the school's network system as soon as possible. Photographs stored on a teacher's personal computer for school

purposes should be deleted as soon as possible after they are no longer required or transferred to the school's C2K system.

Staff, governors, parents and carers must not disclose any information that is confidential to the school or any third party that has disclosed information to the school. That is all written within our Social Media Policy.

Outside Programs and Agencies

Outside programs and agencies will follow this policy to ensure child protection at all times. ICT co-ordinator and Principal to ensure this is clearly explained and monitored.

It is not possible to be certain of the originator of an email message, and for this reason the school is unable to accept an email as parental authorisation of a pupil absence.

Updated: June 2017

Review Date: June 2019