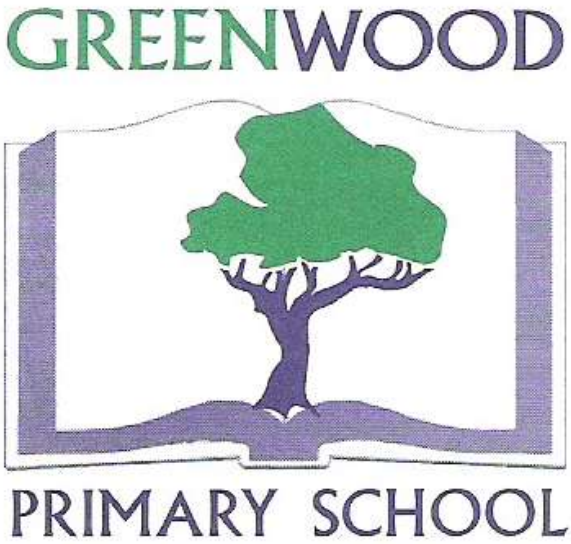
GREENWOOD PRIMARY SCHOOL AND NURSERY UNIT



e-Safety Policy

March 2019

NOTE: Key personnel details – updated September 2019

Greenwood Primary School

e-Safety Policy

1.0 Context

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 Greenwood 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."

2.0 Introduction

- Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning.
- Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.
- In Greenwood Primary School we understand the responsibility to educate our pupils in e-safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. (See ICT Policy)

3.0 What is e-Safety?

e-Safety is short for electronic safety.

This policy highlights the responsibility of the school, staff, governors and parents/carers to mitigate risk through reasonable planning and actions. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology as well as collaboration tools and personal publishing.

e-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

Using the Internet for Education

The benefits include:

- access to a wide variety of educational resources, including online assessment;
- rapid and cost effective communication;
- gaining and understanding of people and cultures around the globe;
- staff professional development through access to new curriculum materials, shared knowledge and practice;
- greatly increased skills in Literacy, particularly in being able to read and appraise critically and then communicate what is important to others;
- social and leisure use.

The internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the internet is an essential skill for children as they grow up in the modern world. The internet is, however, an open communications channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials, some of which could be unsuitable.

Key concerns are:

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons

Children should be taught:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the internet.
- That they should never give out personal details or
- That they should never meet alone anyone contacted via the internet, and
- That once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the internet there are unsuitable materials in many varieties. Anyone can post material on the internet.

Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.

Materials may express extreme views e.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.

Materials may contain misleading and inaccurate information e.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children should be taught:-

- That information on the internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

Excessive Commercialism

The internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

If children are to use the internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave online and to discuss problems. There are no totally effective solutions to problems of internet safety. Teachers, pupils and parents must be vigilant.

The rapidly changing nature of the internet and new technologies means that e-safety is an ever growing and changing area of interest and concern. This e-safety policy reflects this by keeping abreast of the changes taking place. Schools have a duty of care to enable pupils to use on-line systems safely.

This e-safety policy operates in conjunction with other school policies including Positive Behaviour, Child Protection/Safeguarding Children, Anti-Bullying, and the UICT Policy. E-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 Greenwood 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.

3.0 Care and Responsibility

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and encourage awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

All users should have an entitlement to safe internet access at all times. With these opportunities we also have to recognise the risks associated with the internet and related technologies.

The use of these exciting and innovative tools in schools and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers pupils 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;

- cyber-bullying;

- access to unsuitable video/internet games/materials;

- 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.

It is impossible to eliminate the risk completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any scenarios which may arise.

In Greenwood Primary School we understand the responsibility to educate our pupils in e-safety issues. We aim to teach pupils to behave appropriately and think critically, enabling them to remain both safe and within the law when using the internet and related technologies, in and beyond the context of the classroom.

4.0 Roles and Responsibilities

As e-safety is an important aspect of Child Protection/Safeguarding Children within the school, the school's Designated Child Protection Teacher, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT co-ordinator and the e-Safety Team to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. This team has the responsibility for leading and monitoring the implementation of e-safety throughout the school.

The ICT co-ordinator/Principal have the responsibility to update Senior Leadership Team and Governors with regard to e-safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice.

4.1 Responsibilities: ICT Co-ordinator

Our ICT co-ordinator is the person responsible to the Principal and the Board of Governors for the day-to-day issues relating to e-safety.

The ICT co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents;

- will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident;

- provides training and advice for staff;

- liaises with the Education Authority;

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;

- reports regularly to Senior Leadership Team;

- receives appropriate training and support to fulfil her role effectively;

- has responsibility for blocking/unblocking internet sites on C2K;

- passing on requests for blocking/unblocking to the C2K helpdesk;

- maintains records indicating any occasions where the school has used its powers of search and deletion of material on electronic devices (e.g. inappropriate photographs).

4.2 Responsibilities - The Board of Governors:

- are responsible for the approval of this policy and for reviewing its effectiveness. The governors should receive regular information about e-Safety incidents and monitoring reports.

4.3 Responsibilities -The Principal:

- is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety is delegated to the ICT co-ordinator;

- should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. Refer to staff disciplinary procedures, and/or Child Protection/Safeguarding Children Policy.

4.4 Responsibilities - Teaching and Support Staff must:

- have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices;

- embed e-safety issues into the curriculum and other school activities as appropriate;

- have read, understood and signed the school's Acceptable Use of the Internet Policy for staff;

- report any suspected misuse or problem to the school's ICT co-ordinator;

5.0 e-Safety Skills Development for Staff

E-Safety training is an essential element of staff induction and should be part of on-going Continuous Professional Development programme. Through this e-safety policy, we aim to ensure that all reasonable actions are taken and measures put in place to protect all users.

- All staff will receive regular information and training on e-safety issues through the ICT co-ordinator at staff meetings.

- All staff must be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

- All staff are encouraged to incorporate e-safety into their activities and promote awareness within their lessons.

- All staff members will receive a copy of this e-safety policy and Acceptable Use of the Internet Agreement. All staff should read and sign the Acceptable Use of the Internet Agreement.

6.0 Handling of e-Safety

To deal with any incidents of technology misuse by pupils which arise, the school's Positive Behaviour Policy will be followed. Pupils must be made aware the repeated misuse of the internet may lead to their access to it being denied. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed.

Where the incident involves child abuse, the Designated Teacher for Child Protection/Safeguarding Children in the school must be notified and the school will follow procedures as set out in the school's Child Protection/Safeguarding Children Policy.

Issues of internet misuse and access to any inappropriate material by any user should be reported immediately to the school's ICT Co-ordinator and Designated Teacher for Child Protection. Records of the issue and how it was dealt with should be maintained and should include details of the site, the date and the time.

A record of very serious e-safety incidents will be kept in the locked Child Protection/Safeguarding Children cabinet within school.

Harassment of another person using technology, or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), poses a threat to their physical and emotional safety, and may have legal consequences.

For these purposes, it is also essential that evidence of misuse is secured. If the school identifies a suspect device (containing for instance indecent images or offences concerning child protection), it will not be used or viewed and advice will be sought from the P.S.N.I.

After a minor or major incident, a comprehensive debriefing will occur to review school policy and procedures.

Logs of misuse, changes to filtering controls and of filtering incidents are made available to the:

- Senior Leadership Team;
- Principal;
- Governors;
- ICT Co-ordinator.

If police involvement is necessary, the Principal/ICT Co-ordinator/Board of Governors will seek advice from Department of Education and the legal department at the Education Authority (Belfast Region), as appropriate.

7.0 e-Safety Team

The school's e-safety team consists of:

• Miss L Forster	Principal, C2K Manager, Deputy Designated Teacher for Child Protection (Primary)
• Mrs L Caddoo	C2K Manager and ICT Co-ordinator
• Mrs H Lawder	Designated Teacher for Child Protection/Safeguarding (Primary)
• Mrs D Thompson	Deputy Designated Teacher for Child Protection/Safeguarding (Nursery)
• Mrs L McCormick	Designated Governor for Child Protection/Safeguarding

8.0 Illegal or Inappropriate Activities

The school believes that the activities listed below are inappropriate (and on occasions illegal) in a school context and that users should not engage in these activities when using school equipment or systems (in or out of school). 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;
- 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.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. 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 that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

9.0 e-Safety and Pupils

Pupils need to know how to cope if they come across inappropriate material or situations online. e-Safety will be discussed with pupils on an ongoing and regular basis. This should be discussed with the pupils in an age appropriate way as a set of rules that will keep everyone safe when using technology in school.

Activities to promote e-safety awareness are taught throughout the school year and include participation in Safer Internet Day.

All children will follow a progressive online safety curriculum aimed at ensuring that they are equipped with the skills to keep them safe online and make them responsible digital citizens both now and in the future.

The e-safety curriculum being followed is the collaborative work of the East Belfast Primary ICT Cluster group with guidance from the UK Council for Child Internet Safety.

10.0 e-Safety and Staff

Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Regard should be given to the school's staff Code of Conduct, the school's e-Safety Policy and ICT Acceptable Use Policy at all times both inside and outside of work.

All staff will be introduced to the e-Safety Policy and its importance explained. Staff will be asked to read and sign the Acceptable Use of the Internet Agreement for Staff which focuses on e-safety responsibilities in accordance with the Staff Code of Conduct. Staff should be aware that all Internet traffic (including email) is monitored, recorded and tracked by the C2K.

Staff using their own digital cameras or mobile telephones in exceptional circumstances to take photographs or video footage should transfer the images/footage as soon as possible to the school's C2K system and then delete them from the camera, mobile phone or similar device.

Staff have access to 'YouTube' (for educational purposes only) when logged into the C2K system. Therefore, staff must ensure that no pupil is given access to a computer that they are logged on to unless being supervised.

Staff should always ensure that any Internet searches involving sites that have been granted enhanced access to should not be carried out when children can view them, i.e. on the computer's screen or on an interactive whiteboard. 'YouTube' should only be used after the content has been viewed and checked, ensuring that children are not exposed to inappropriate content.

11.0 e-Safety and Parents/Carers

The e-Safety policy will be published on the school's website and parents/carers will be encouraged to read the document. Greenwood Primary School will look to promote e-Safety awareness within the school community which may take the form of information evenings for parents/carers, information leaflets and/or links on the school website.

Information is available on the 'Think U Know website': www.thinkuknow.co.uk

12.0 Internet Security – C2K

Staff and pupils accessing the Internet via the C2k Education Network will be required to authenticate using their C2k username and password. This authentication will provide Internet filtering via the C2k Education Network solution.

Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school Principal.

Connection of non C2K devices to the Internet e.g. iPads and other personal devices is through the controlled C2K guest wireless network and is subject to the C2K filtering service.

13.0 Internet Use

- The school will plan and provide opportunities within a range of curriculum areas to teach e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside of school will be discussed with pupils in an age appropriate way on a regular basis by teachers.
- Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of how to seek advice or help if they experience problems when online e.g. from a parent/carer, teacher/trusted member of staff.
- The school internet access is filtered through the C2K managed service.

- No filtering service is 100% effective, therefore all children's use of the Internet is supervised by an adult.

- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the internet in response to a need e.g. a question which has arisen from work in class.

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

- Children will be taught to be 'Internet Wise' and therefore good online citizens and are encouraged to discuss how to cope if they come across inappropriate content.

15.0 School Website

Greenwood Primary School's website 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 being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions;

- Only photographs of children with parent/carer consent will appear on the school's website.

- Names will not 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 includes school telephone number, school address and general email address.

16.0 Social Networking

Social software is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs (personal web journals).

Social environments enable any community to share resources and ideas amongst users. There are many excellent public examples of social software being used to support formal and informal educational practice amongst young people and amongst educators. They are also popular ways of enabling users to publish and share information, including photographs, video from webcams, video files and blogs about themselves and their interests.

Given the age profile of the school, our children are too young to access and use social media sites. The school does not have or promote the use of social media sites.

Social networking through the use of internet-based and other electronic social media tools is integrated into everyday life. Use of Facebook, Twitter, blogging, wikis and other online social media vehicles are now commonplace with the result that the lines between work and personal life can become blurred. To protect staff, pupils and the reputation of the school the following guidelines should be followed:

- Staff should not use school systems to engage in personal social media activities, i.e. Facebook, Twitter, blogging, wikis etc. This inappropriate use of social media sites may be treated as a disciplinary matter;

- If staff use social media sites for personal use, they are reminded that they have a responsibility to ensure they are posting comments or images that are not detrimental to their position as a staff member of Greenwood Primary School, the privacy or rights of pupils or the reputation of the school. Images may include photographs from staff parties that could be misinterpreted and present the staff or the school, in a negative light. A common sense approach to the use of social media websites is recommended.

17.0 Password Security

- Staff users are provided with an individual login username and password. Passwords are changed in line with C2K policy and requirements. Login details should not be shared with pupils, and should be changed if it appears pupils have worked out an adult's password.

- Pupils are provided with an individual login username and password.

- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.

- Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

18.0 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.

Given the age profile of the school, our children should not have unsupervised access to the internet and should not be present on social media sites.

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. Pupils/parents are also encouraged to click the 'Report Abuse' link which is available on social media

A record is kept of all incidents of cyber-bullying. 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.

19.0 Network Access

Pupil and staff access to the internet using school electronic equipment is through a filtered service provided by C2K which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse.

Pupils must not use any personal electronic devices within school to access the internet or any messaging services without prior permission from a member of staff.

20.0 Acceptable Internet Use Policy for Staff

The C2K computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's e-Safety policy has been drawn up to protect all parties – the pupils, the staff and the school.

The school reserves the right to examine and delete any files that may be held on its computer system or to monitor any Internet sites visited. Staff should read and sign a copy of the school's Acceptable Internet Use Agreement for Staff and return it to the Principal. (See UICT Policy)

21.0 Mobile Technologies

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on personal memory sticks. If information is to be stored on a USB pen, staff must use an encrypted version provided by the school. An Acceptable Use agreement must be completed. Staff must recognise that they are responsible for the safekeeping of the USB pen in line with safeguarding and GPDR requirements.
- Pupils are not allowed to use personal mobile devices/phones (in school) during class.
- Staff should not use personal mobile phones during designated teaching sessions.

22.0 Managing Video-Conferencing

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

23.0 Handling e-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator. Records of the incident will be maintained.
- Any complaint about staff misuse must be referred to the ICT Co-ordinator and/or Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection/safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure. This is available on the school website and from the school office.

23.0 Related Policies

- ICT
- Positive Behaviour
- Anti-Bullying
- Safeguarding/Child Protection
- Pastoral Care

24.0 Policy Review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually or more frequently if required. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

(Date of Next Review: March 2020)

Signed: _____ Principal

Signed: _____ Chair, Board of Governors

Date: _____

Ratified by Board of Governors: **6th March 2019**

Original signed copy held in Principal's Office.

Appendix 1


Stay Safe Online
Remember the 5 SMART rules when using the internet and mobile phones.
S
SAFE: Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.
m
MEET: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING: Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE: Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.
t
TELL: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
Find out more at Childnet's website ...
www.kidsmart.org.uk
Childnet International © 2002-2010 Registered Charity no. 1080173 www.childnet.com
Childnet International
KidSMART

Appendix 2

Internet Streaming – Acceptable use Agreement
Overview

The new C2k Education Network introduces a revised system for internet filtering based on a Websense filtering solution. Websense assesses all websites based on their content and adds them to a category. Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.

Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.

What's Different?
Previously, primary schools had no school control over the internet sites available, and post primary and special schools had access to a number of internet "amber groups" to which users could be added. The new system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

School choice:
In addition to the default sites, schools can choose to make users members of one or more internet-related security groups. These are:

- Internet Social Networking
- Internet Streaming Media
- Internet Advanced

Access to these groups is controlled by the C2k Manager who can add individual users or groups of users to these groups via the Identity Management tool in MY-SCHOOL.

Internet Streaming
This group provides access to YouTube, BBC iPlayer, Vimeo and other television and radio streaming sites. When a user is added to the Internet Streaming security group the following categories, RED in the Default policy, are now GREEN.

Greenwood Primary School Implications
If a member of staff is to be added to the Internet Streaming groups they must agree to the following:

- To check all video that is to be shown to classes before use
- Be responsible for the content of any video shown to a class
- To use in an appropriate manner and in accordance with the guidelines detailed in the school's E-Safety Policy and Child Protection Policy

I agree to the terms of the Internet Streaming Acceptable Use Agreement and wish to be added to this group.

Signed _____ Date _____

Appendix 3

Advanced Internet Streaming – Acceptable use Agreement Overview

The new C2k Education Network introduces a revised system for internet filtering based on a Websense filtering solution. Websense assesses all websites based on their content and adds them to a category. Through the C2k service, categories of sites can be made available to users, while access to other categories will be restricted. Access to the most inappropriate sites, including those on the Internet Watch Foundation banned list will always remain blocked.

Note: The same C2k filtering applies across the C2k network, whether using a C2k core desktop computer or a personal iPad. This consistency is essential to ensure the safety and integrity of C2k's internet provision.

What's Different?

Previously, primary schools had no school control over the internet sites available, and post primary and special schools had access to a number of internet "amber groups" to which users could be added. The new system categorises all websites as either red (unavailable) or green (available). By default, all users are given access to a core set of green sites.

School choice:
In addition to the default sites, schools can choose to make users members of one or more internet-related security groups. These are:

- Internet Social Networking
- Internet Streaming Media
- Internet Advanced

Access to these groups is controlled by the C2k Manager who can add individual users or groups of users to these groups via the Identity Management tool in MY-SCHOOL.

Internet Advanced

This group provides access to a range of websites that contain adult material. These include: webmail, shopping, drugs and alcohol, sex education. When a user is added to the Internet Advanced security group these categories, RED in the Default policy, are now GREEN. A full list of categories can be found on information sheet E039

Greenwood Primary School Implications

If a member of staff is to be added to the Internet Advanced groups they must agree to the following:

- To check all websites before they are shown to classes
- Be responsible for the content of any websites shown to a class
- To use in an appropriate manner and in accordance with the guidelines detailed in the school's E-Safety Policy and Child Protection Policy
-

I agree to the terms of the Internet Advanced Acceptable Use Agreement and wish to be added to this group.

Signed _____ Date _____

Appendix 4

GREENWOOD PRIMARY SCHOOL AND NURSERY UNIT

USE OF DIGITAL IMAGES: PARENTAL PERMISSION AGREEMENT

Dear Parent/Guardian,

During the course of your child's education at Greenwood Primary School and Nursery Unit, digital cameras will be used as part of recording activities for various purposes. Taking, keeping and publishing photographs and video footage involves processing personal data under data protection laws.

To enable us to comply with our obligations under the General Data Protection Regulation, we are required to obtain express consent for the use of a pupil's image for example in school displays, in newsletters, on the school website.

Please read the information below and then indicate, on the attached form, whether consent is given or not for your child to be included in the various activities.

1. Individual and/or group photographs of classroom activities for display in either the classroom or the school corridor/hall. e.g. P1 children during play based learning, history costumes worn by P3 children, children as part of a timeline, school trips to the farm. (Individual names may be used beside photographs.)
2. Individual and/or group photographs which may be included in the school prospectus and other printed publications which we may produce for promotional purposes. e.g. posters to advertise the school's annual Open Day. (Individual names will not be used beside photographs.)
3. Individual and/or group photographs for use on the school website including individual achievements and/or school events. e.g. Celebrating school events such as Christmas performances or P3 Leavers' Concert, showcasing class learning, as part of a school newsletter. (Individual names will not be used beside photographs.)
4. Individual and/or group photographs/television coverage of school events for publicity in local press/TV. (Individual names will not be used beside photographs.)
5. Individual and/or group video clips for use in school. e.g. for Curriculum Information Meetings for parents, a video of a reading group, a video of play based learning, a video celebrating outdoor learning day.

Consent is given for the duration of your child's attendance at Greenwood Primary School and Nursery Unit or until you inform the school otherwise. If any variations to these consents arise parents will be contacted regarding use of the digital image.

Consent can be withdrawn at any time by notifying the Principal and completing a new copy of this form. If you do not consent to a particular use of your child's digital image, this will not adversely affect you in any way. Where you would like to amend the provisions for which consent has been provided, you should submit your request in writing to the Principal. A new form will be issued to you to amend accordingly.

If you have any queries regarding the use of photographs/digital images, with which I can be of assistance, please do not hesitate to contact me at school.

Yours sincerely

USE OF DIGITAL IMAGES: PARENTAL CONSENT AGREEMENT

CONSENT FORM

Please ensure you read each request and clearly indicate whether consent is given or not.

Please ✓ to indicate that you **are giving consent** or ✗ to indicate that you **are not giving consent**.

☐ ✓ or ✗

1. Individual and/or group photographs of classroom activities for display in either the classroom or the school corridor/hall. e.g. P1 children during play based learning, history costumes worn by P3 children, children as part of a timeline, school trips to the farm. (Individual names may be used beside photographs.)

☐ 2. Individual and/or group photographs which may be included in the school prospectus and other printed publications which we may produce for promotional purposes. e.g. posters to advertise the school's annual Open Day. (Individual names will not be used beside photographs.)

☐ 3. Individual and/or group photographs for use on the school website including individual achievements and/or school events. e.g. Celebrating school events such as Christmas performances or P3 Leavers' Concert, showcasing class learning, as part of a school newsletter. (Individual names will not be used beside photographs.)

☐ 4. Individual and/or group photographs/television coverage of school events for publicity in local press/TV. (Individual names will not be used beside photographs.)

☐ 5. Individual and/or group video clips for use in school. e.g. for Curriculum Information Meetings for parents, a video of a reading group, a video of play based learning, a video celebrating outdoor learning day.

Consent is given for the duration of your child's attendance at Greenwood Primary School and Nursery Unit or until you inform the school otherwise.

If any variations to these consents arise parents will be contacted regarding use of the digital image.

Child's Name: _____ Class: _____

Signed: _____ Date: _____

(Parent/Guardian)