E-Safety Policy

And

Acceptable Use Agreements

January 2022

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

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 Lisburn Central 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.

The Internet

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.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, 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 to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal/ICT Co-ordinator will update Senior Management and Governors with regard to e-safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, PDMU, Health and Safety/Risk Assessment, Child Protection, Anti-bullying and Code of Conduct for teaching and non-teaching staff.

It has been agreed by the Senior Management Team, Staff and approved by the Governing Body. The e-Safety policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings.
- All staff have been 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.
- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- The school will communicate relevant e-Safety information through newsletters and the school website.
- 'Share Aware' sessions for parents will be held by outside agencies to communicate relevant and up-to-date e-Safety information.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

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 school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service and SSNi 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.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted. Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. The teacher supervises messages sent and received in this way.

Social Networking:

- The school C2k system will block access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

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 memory sticks.
- 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.

Managing Video-conferencing:

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

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.

- Photographs of individual pupils will not be permitted. Only pictures of groups or group activities will be used.

- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All 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 are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

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, reported to the Safeguarding team, recorded in the incident logbook and dealt with accordingly.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints' procedure.

Communicating the Policy:

Introducing the e-Safety Policy to pupils

- e-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored**.**
- Outside agencies reinforce e-Safety messages with pupils.

Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop or iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

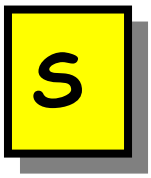
Monitoring and review:

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

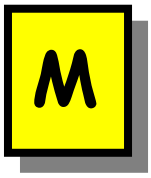
This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

Safety Rules for Children

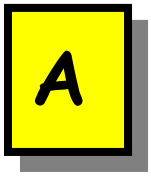
Follow These SMART TIPS



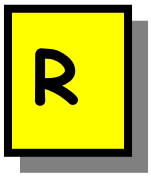
Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!



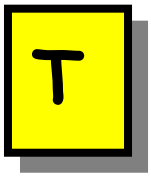
Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.



Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees

LISBURN CENTRAL PRIMARY SCHOOL
Acceptable Use of the Internet

The school has installed computers, iPads and Internet access to help in teaching and learning. These rules will keep everyone safe and help us be fair to others. Parents and children must be aware of these rules and agree to follow them.

- I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will not bring USB devices into school unless I have been given permission.
- I will ask permission from a member of staff before using the internet.
- I will use the Internet for research and school purposes only.
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and sensible.
- I will make sure my comments on Seesaw are polite and sensible.
- I will not give my name, address or phone number or arrange to meet someone, unless my parent, carer or teacher has given permission.
- I will respect the privacy of others. I will not give out names, address, phone numbers or photographs.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers, unless instructed to do so by the teacher.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that I store files and documents that are password protected, on Google Drive that I can access through the teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I understand that if I deliberately break these rules I may not be allowed to use the Internet and/or the computers/iPads.

LISBURN CENTRAL PRIMARY SCHOOL

Rules for Responsible Internet Use
Foundation Stage

The school has installed computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- **I will listen to what my teacher asks me to do and use the computer sensibly.**

PUPIL signature: _____ Date _____

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the school computers. I have read the above stated rules for use of the school computer, iPad, school network and Internet and accept responsibility for setting and conveying appropriate standards for my child.

Parent/Guardian signature: _____ Date: _____

Print name of pupil: _____ Class: _____

LISBURN CENTRAL PRIMARY SCHOOL

Rules for Responsible Internet Use
Key Stage 1

The school has installed computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- **I will use my own login username and password.**
- **I will not open, change or delete anything without asking.**
- **I will not download any software or apps.**
- **I will not open other people's files or change their work.**
- **I will only use the computers for school work and homework.**
- **I will ask before using the Internet.**
- **I will not give my home address or telephone number.**
- **I will not give out names, addresses, phone numbers or photographs.**
- **I will tell a teacher if I see anything I am unhappy with.**
- **I will make sure my comments on Seesaw are polite and sensible.**
- **I understand that the school may check what I do on the computer.**
- **I understand that if I deliberately damage a school computer or iPad my parents will be responsible for repairing this.**
- **I understand that if I deliberately break these rules, I may not be allowed to use the Internet and/ or the school computers and iPads.**

PUPIL signature: _____ Date _____

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the school computers. I have read the above stated rules for use of the school computer, iPad, school network and Internet and accept responsibility for setting and conveying appropriate standards for my child.

Parent/Guardian signature: _____ Date: _____

Print name of pupil: _____ Class: _____

LISBURN CENTRAL PRIMARY SCHOOL

Rules for Responsible Internet Use – Key Stage 2

The school has installed computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- **I will only use my own login username and password.**
- **I will keep my username and password private.**
- **I will not access other people's files without their permission.**
- **I will not change or delete other people's work/files.**
- **I will not bring USB devices into school unless I have been given permission.**
- **I will ask permission from a member of staff before using the internet.**
- **I will use the Internet for research and school purposes only.**
- **I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and sensible**
- **I will make sure my comments on Seesaw are polite and sensible.**
- **I will not give my name, address or phone number or arrange to meet someone, unless my parent, carer or teacher has given permission.**
- **I will respect the privacy of others. I will not give out names, address, phone numbers or photographs.**
- **I understand that I am not allowed to enter Internet Chat Rooms while using school computers.**
- **If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I understand that I store files and documents that are password protected, on Google Drive that I can access through the teacher.**
- **I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.**
- **I understand that if I deliberately damage a school computer or iPad my parents will be responsible for repairing this.**
- **I understand that if I deliberately break these rules I may not be allowed to use the Internet and/or the computers and iPads.**

Pupil signature: _____ Date _____

As the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the school computers. I have read the above stated rules for use of the school computer, iPad, school network and Internet and accept responsibility for setting and conveying appropriate standards for my child.

Parent/Guardian signature: _____ Date: _____

Print name of pupil: _____ Class: _____

LISBURN CENTRAL PRIMARY SCHOOL

Acceptable Use Agreement
For Staff

The 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 Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

I agree to the terms of the Acceptable Use Agreement.

Name: _____ **Signature:** _____

Date: _____

Internet Streaming
Acceptable use Agreement

Overview
The 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 is 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 C2k 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.

Lisburn Central 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 Online 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 _____

Lisburn Central Primary School

iPad User Agreement and Acceptable Use Policy

General Information

iPads allocated to teachers are the property of the School and should be looked after with appropriate care. Teacher use of the iPad falls under the School's ICT Policy, its Child Protection Policy and the Online Safety Policy.

Using the IPad

The School's ICT team will initially set up the iPad in a way that best suits your classroom and these settings should not be changed by staff. Use of the iPad will require a few necessary tasks to keep the device performing well. These are:

- Clean the screen often with approved cleaning towels
- keep away from food and drink
- Charge the iPads only with the included charger standard wall outlet for your power source or Multidock charger.

Any errors or problems with the iPad should be reported to the School's ICT team as soon as possible.

Staff should sign a copy of this Acceptable Use of iPads Agreement and return it to the Principal.

Staff agree to

- Use iPads for educational purposes only.
- Follow the school's ICT Policy, Child Protection Policy and the e-Safety Policy at all times.
- Abide by the school's Acceptable Use of the internet policy with regards to iPad usage.
- Back up data securely by saving documents, videos and photos to their school Google Drive account or another of the Lisburn Central P.S accounts they have access to.
- Install a four-digit PIN on their staff iPad and provide this on demand to the school management team.
- Keep the PIN for their staff iPad secure and not divulge it to pupils.
- Only download 'Apps' to iPads that have been purchased through the school iTunes account by a member of the ICT team.

- Request through the ICT Co-ordinator any additional 'Apps' they would like to be added for educational purposes. Where these are agreed they will be downloaded via the school's iTunes account and made available for download onto every iPad.

- Not install apps that may be considered only for staff personal use, or would be deemed unsuitable for the classroom.

- Keep iPads 'out of sight' when not in use.

- Report loss, theft or damage to the school's ICT team immediately.

- Take full responsibility for loss, theft or damage of an iPad if they take the iPad home. In the event of loss, theft or damage occurring outside of school, the member of staff has the responsibility for ensuring the iPad is covered under their insurance policy.

I understand and will abide by the use of iPad regulations outlined above, in conjunction with the school's ICT Policy, E-Safety Policy and Child Protection Policy. I further understand that should I commit any violation the School may ask me to return the iPads and school disciplinary or legal action may ensue. I agree to periodically hand in my iPads for routine maintenance, security up-dating and screening.

Name: _____ Signature: _____

Date: _____