All Children's Integrated Primary School

Acceptable Use of Internet / e-Safety Policy

Policy to be ratified by BoG in 2026-2027

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 All Children's IPS 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."

WHAT IS e-SAFETY?

e-Safety is short for electronic safety. This policy highlights the responsibility of the school, staff, governors and parents 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;
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

USING THE INTERNET FOR EDUCATION

Benefits include:

- access to a wide variety of educational resources; including online assessment:
- rapid and cost effective communication;
- gaining an 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.

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, Mobile Phone and other related technologies. 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 All Children's IPS 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

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 stimulate 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 All Children's IPS 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.

ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of Child Protection/Safeguarding Children within the school therefore, the school's ICT Co-ordinator, Safe-guarding/Child Protection Team, 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 Safeguarding/Child Protection 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 (as DT) 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.

Responsibilities: ICT Co-ordinator

Our ICT coordinator 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:

- leads the e-Safety team as well as discussions on e-Safety with the School Council and takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents;
- ensures 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 his/her role effectively;
- has responsibility for blocking/unblocking internet sites on C2k;
- passing on requests for blocking/unblocking to the C2K helpdesks;
- *maintains the e-Safety Log Book indicating any occasions where the school has used its powers of search and deletion of material on electronic devices (E.g. inappropriate photographs).

Responsibilities - The Board of Governors:

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.

Responsibilities -The Principal

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;
- is responsible for ensuring that the Vice-Principal 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)

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 e-Safety co-ordinator;

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.

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 e-Safety Co-ordinator and recorded in the school's e-Safety log, giving details of the site and the time.

A record of very serious 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:

- Safe-guarding/Child Protection Team
- Senior Leadership Team;
- Principal;
- Governors or governors' sub-committee;

If police involvement is necessary, the Principal/ICT Co-ordinator/Board of Governors will seek advice from Schools' Branch and the legal department at the Education Authority (South Eastern Region).

Safeguarding/Child Protection Team

The school's Safeguarding/Child Protection Team consists of:

Mr J Beattie	Principal & DT
Mr M Houlahan	ICT Co-ordinator, C2k Manager and DDT
Mr D George	Designate Governor for Safeguarding/Child Protection
Mrs G Gleghorn	Chairperson of BoG

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 as follows:

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. We have a comprehensive programme of lessons from the NSPCC Keeping Safe programme which teach about the importance of online safety.

Activities throughout the school year including Safer Internet Day, drama productions sponsored by the Safeguarding Board and visits from the PSNI (Bee Safe) will reinforce e-Safety and further pupils' understanding.

e-SAFETY AND STAFF

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 systems.

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 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.

Staff encouraged to refer to Safer Schools app for alerts and online safety issues (DENI and Safer Schools Partnership).

e-SAFETY AND PARENTS

The e-Safety policy will be published on the school's website and parents will be encouraged to read the document. All Children's IPS 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.thinkyouknow.co.uk

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 same level of filtering as the main school system.

INTERNET USE

- The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety ie NSPCC Keeping Safe programme
- 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 and other agencies (as appropriate – e.g. NSPCC workshops on online safety).
- 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/carers, teacher/trusted member of staff. Uberheroes workshops deals with online bullying.
- The school internet access is filtered through the C2K managed service;
- 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 to use the internet as an aid to learning.
- 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.

E-MAIL USE

- C2k recommends that all staff and pupils should be encouraged to use their C2k email system for school business. It is strongly advised that staff should not use personal email accounts for school business.
- The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.
- Pupils must immediately tell a teacher when using their C2K email address (if activated) if they receive an 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 by staff or pupils is not permitted.
- Children will not always be given individual C2K e-mail addresses. In some instances, children may have access to a group e-mail to communicate with other children as part of a particular project. Messages sent and received in this way will be supervised by the teacher.
- Children will send work to teachers via the Google Classroom platform, therefore, all correspondence can be facilitated using Google Classroom.

SCHOOL WEBSITE / SCHOOL APP

All Children's IPS's website and app 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 parental/carer consent will appear on the school's website.
- Names will be included with photographs on the website only if parent/carer permission has been given;
- 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.

SOCIAL MEDIA

To keep safe online, young people need to understand the role of social media in the offline world. It's key for pupils to know that their actions online can have very real consequences offline. Pupils also need to be aware of the role of influencers with an online social media presence. Fake news can also be a problem for pupils online and can result in false reporting, misinformation, spin, conspiracy theories and reporting that some people disagree with. Pupils need to be aware of harmful content on social media which could include live news, violence, sexualised content and the incitement of activities that can harm young people both physical and emotionally. It is important that pupils are aware that almost all interactive social media apps, websites and other platforms have guidelines or rules for use which can be used to report inappropriate or distressing content.

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.

C2k filters out services which are misused and block attempts to circumvent the filters. Pupils will not be allowed to use any social software which has not been approved by teaching staff and the C2K filtering service.

Staff and pupils are advised that it is not acceptable or school policy for them to be friends on social network sites (e.g. Facebook). Pupils in this school are told they should not request to be friends with a member of staff on a social network site. Equally, staff are also told that they must not request to be friends or accept requests to be friends with pupils or past pupils of the school on any such site. This is good practice in line with child protection/safeguarding children policy.

- The school C2K systems deny access to social networking sites
- Pupils and their parents/carers are 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.
- Cyber-bullying is addressed within this policy and staff are made aware that pupils may be subject to cyber-bullying via electronic methods of communication both in and out of school. (More information provided below).
- Our pupils are asked to report any incidents of cyber-bullying to the school.

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 All Children's IPS, 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.

PASSWORD SECURITY

- Staff 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, and should be changed if it appears pupils have worked out an adult's password.
- 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 Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

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 All Children's IPS has a specific policy on the acceptable use of mobile phones and related technologies.

If mobile phones or other related technologies are brought into school by pupils, it is our policy that they should remain switched off during the time the 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.

Access to the Internet on such non C2K devices for school related business only be granted using the C2K guest access and therefore is subject to C2K's filtering service.

Staff members can log in to the Google Classroom platform from home using the C2K login password.

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.

NETWORK ACCESS

Pupil and Staff access to the Internet 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.

WORKING AT HOME

The following guidance is relevant to any member of staff working at home.

- Work directly from/to the C2k My-School network (www.c2kschools.net) by logging on with user's C2k credentials; This reduces the need to take electronic information via a USB pen or other media outside of school.
- Staff who are members of SIMS Remote Access Group can access SIMS remotely from a managed laptop (https://remote.c2kschools.net) by logging on with their SIMS credentials. (EN088)
- While working on a C2k laptop, do not use the local "C" drive to store information as locally stored files are not backed up and will be lost in the event of a rebuild. Instead, log in to My-School and work directly with documents from the My Files folder on the C2k Network. Data saved in My Files is backed up.
- Ensure that the C2k laptop and applications are up to date with virus protection software and security patches by connecting them to the C2k Network once a week
- The C2k email account is a DE provided professional mailbox, and should be used for all work related communications. The C2k email account is accessible via the Internet (www.c2kschools.net)
- No external agency or support service should be allowed to tamper with the C2k laptops hardware or software.
- Take care when transporting information/devices to and from home.
- If travelling by public transport hold onto the laptop rather than placing it on a luggage rack. Laptops must be carried in a laptop bag or rucksack.
- If travelling by car, lock the laptop in the boot. Do not leave it in plain sight.
- When working at home, security should be of the same standard as that which is provided in the school.

- Logging out - Outside school: All users should "Log out" of C2k services when their work is complete or when stepping away from the device. This good practice is a standard security measure which will prevent unauthorised access to a user's MyFiles, Fronter, C2k email and SIMs.
- Do not use personal, non-C2k desktop, laptop or other devices to store sensitive school information. Instead, use the remote C2k access to My-School, My-Files, Sims & Private Folders.
- If data has been saved locally to a non-C2k device:
  (i) data could be accessed if the device is stolen
  (ii) it is important to make arrangements to ensure that the school related data is no longer available when the device is being disposed of.
  (iii) If school information is regularly accessed on a home computer, the home user should create a password protected account that is exclusively used by them for work. This restricts accidental access to school information by other home users of the computer.

DATA PROTECTION: GDPR

A failure to safeguard personal data at home could breach the General Data Protection Regulation (GDPR). In addition to financial penalties, a data protection breach could cause serious harm to the school's reputation and damage its relationship with a range of stakeholders including potential students and parents.

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 students, 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.

POLICY REVIEW

This e-Safety policy and its implementation will be reviewed annually or updated when new technologies are introduced and after a risk assessment has been completed.

RELATED POLICIES

- Positive Behaviour
- Anti-Bullying
- Child Protection/Safeguarding Children
- Use of Mobile Phones
- Pastoral Care

ACCEPTABLE INTERNET USE AGREEMENT FOR STAFF/VOLUNTEERS

STAFF MEMBER: _____

In line with All Children's IPS Use of Internet/e-Safety policy I understand:

- I must not engage in any on-line activity that may compromise my professional responsibilities or bring the name of the school into disrepute;

- the school has the right to monitor my use of the school's ICT systems, email and other digital communications;
- I will not search for, access, upload, download any materials which are inappropriate/illegal such as child sexual abuse images pornography, racist, sectarian or offensive material is forbidden;
- I must immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Principal or the school's e-Safety co-ordinator;
- the use of school ICT systems for personal financial gain, gambling, political purposes or advertising is forbidden;
- I must not disclose my C2K username or password to anyone else, nor will I try to use anyone else's C2K username and password;
- I will not use the school systems to access social media sites and I will not make friend requests to pupils or accept friend requests from pupils;
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of photographs/digital images;
- I must not access, copy, remove or otherwise alter any other user's files, without their express permission; any activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- when communicating electronically with others I should be professional, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
- posting anonymous messages and forwarding chain letters is forbidden;
- the need to be cautious when opening attachments to emails, due to the risk of the attachment containing viruses or other harmful programmes;
- copyright of materials must be respected;
- that this Acceptable Use of the Internet Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school;
- the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the context of the school's e-Safety policy;
- I will only use my personal mobile ICT devices as agreed in the school's 'e-Safety Policy' and the school's 'Use of Mobile Phones and Related Technologies Policy';
- I should immediately report any damage or faults involving equipment or software, however this may have happened;
- when using the C2K there is a log of my Internet searching history.

I understand that if I fail to comply with this Acceptable Internet Use Policy Agreement. I could be subject to disciplinary action, referred to the P.S.N.I. for further investigation and/or the procedures followed in line with the school's Child Protection/Safeguarding Children Policy.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Signed: _____ Date: _____

ACCEPTABLE USE OF THE INTERNET: GUIDELINES for PUPILS

Children should be taught from P1 – P7 that they are responsible for their use on the Internet in school and that they should use it in a safe, responsible and appropriate manner. The following guidelines are shared and discussed with the pupils in an age appropriate way.

Staff should continually teach and stress the importance of safe use of the internet.

WHEN USING THE C2K SYSTEM PUPILS SHOULD:

- only use their own login username and password;
- use the Internet for school/educational purposes only;
- tell a teacher immediately if he/she sees anything that they consider inappropriate or receive messages they do not like;
- only send e-mail or any other form of electronic communication in school when directed by the teacher;
- make sure any internet based communication is polite and responsible;
- understand that if they consistently choose not to comply with these expectations they will be warned and subsequently may be denied access to Internet resources;
- understand that the school may check their computer files/e-mails and may monitor the Internet sites that they visit when on school systems.

USING THE C2K SYSTEM PUPILS SHOULD NEVER:

- access other people's files without their permission;
- change or delete other people's work/files without their permission;
- provide personal information such as telephone numbers and addresses when using the Internet;
- electronic communication to arrange to meet anyone;
- use Social Media or equivalent while in school;
- bring in memory devices from home to use in school unless given permission by a member of staff;
- use any personal electronic devices they have their possession within school to access the internet or any messaging services unless permission has been given by a member of staff.