GLENGORMLEY INTEGRATED PRIMARY SCHOOL

Online Safety Policy

Schedule for Developing, Monitoring and Reviewing Policy

Approval by the Board of Governors:	May 2019
The implementation of this Online Safety Policy will be monitored by:	Principal and SLT Safeguarding Team Online Safety Leader
Monitoring and Reviewing:	Biannually or as required following any change to ICT provision for staff or breach of the policy.

Glengormley Integrated Primary School
Online Safety Policy

This Online Safety policy operates in conjunction with other school policies:

- *Safeguarding and Child Protection;*
- ICT policy;
- Positive Behaviour;
- *Anti-Bullying;*
- *Mobile Phones and Related Technologies;*
- Staff Code of Conduct.

Online safety must be built into the delivery of the curriculum, forming a core element of the school's Safeguarding and Child Protection policy. DENI Circular 2019/08, '*Child Protection: Record Keeping in Schools*' defines safeguarding as more than child protection. It defines it as beginning with promotion and preventative activity that enables children and young people to grow up safely and securely without adverse effect to their development and wellbeing. Integral to this is the support of families and early intervention to meet the needs of all children and young people.

As such, this policy highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. It also includes the school's approaches to support families in their awareness of online safety issues and the promotion of responsible and safe online use at home.

Online Safety in Glengormley Integrated Primary School depends on effective practice at several levels:

- the responsible use of ICT by all staff and children; encouraged by education and made explicit through published policies;

- sound implementation of the Online Safety Policy in both administration and curriculum, including secure school network design and use;

- the safe and secure provision of internet access through the DE funded C2K Managed Service, including C2K Wireless network access.

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 Circular 2011/22 and 2013/25 on Internet/Online Safety. This document sets out the policy and practices for the safe and effective use of the internet and related technologies in Glengormley Integrated Primary School. It also links to Article 17 from the UN Convention on the Rights of the Child which states that:

"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."

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years and there is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Glengormley Integrated Primary School has made a significant investment both financially and physically to ensure these technologies are available to our learners. The benefits are perceived to "outweigh the risks", however, we must, through our Online Safety policy, ensure that our provision for online safety meets the statutory obligations to ensure that children and young people are safe and are protected from potential harm; both within and outside school.

1.0 – Introduction

1.1 - What is Online Safety?

This policy highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. Online 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.

Online 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 helping children recognise unsafe situations and how to respond to risks appropriately.

1.2 - Writing and Reviewing Online Safety

The Online Safety policy is part of the School Development Plan and relates to other policies including those for ICT and for Safeguarding and Child Protection.

- The school will appoint an Online Safety Coordinator. This role is currently fulfilled by Mark Donaghy.
- Our Online Safety Policy has been written, building on guidance provided through the DENI Circular 2013/25. It has been agreed by the senior management and approved by governors.
- The Online Safety Policy will be reviewed by the Board of Governors biannually or

as required due to a change in ICT provision or a breach of the policy.

2.0 – The Use of the Internet in Teaching and Learning (E-Learning)

2.1 – The Importance of Internet Use

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children.

2.2 – Whole School Approach to Online Safety

- The school will plan and provide opportunities within a range of curriculum areas to teach Online Safety.
- Educating children on the dangers of technologies that may be encountered outside of school will be discussed with children in an age appropriate way on a regular basis by teachers and other agencies as appropriate.
- Children will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Children will also be aware of how to seek advice or help if they experience problems when online. The issue of Cyberbullying is referred to later in this policy;
- The school's internet access is filtered through the C2K managed service;
- The school's internet access is expressly for child and teacher use and includes filtering appropriate to the age of children;
- Children will be taught what internet use is acceptable and what is not and will be given clear objectives for internet use. They will be encouraged to discuss how to deal with situations where they may come across inappropriate content;
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of children;
- Staff should guide children in online activities that will support the learning outcomes planned for the children's age and maturity.

2.3 – Online Safety and Children

Children need to know how to behave if they come across inappropriate material or situations online. Online Safety will be discussed with children on an ongoing and regular basis. This should be discussed with the children in an age appropriate way as a set of rules that will keep everyone safe when using technology in school. **See Acceptable Use Policy for Children (Appendix 1a/b).**

Activities throughout the school year, including Internet Safety Week and visits from outside agencies, such as the PSNI, Antrim & Newtownabbey Borough Council, NSPCC, along with whole school assemblies led by staff and the KS2 Digital Leaders, will reinforce Online Safety and further children's understanding.

- If staff or children discover unsuitable sites, the URL (address), time, date and content must be reported to the school Online Safety Coordinator and in turn, C2k.
- Schools should ensure that the use of internet derived materials by staff and by children complies with copyright law. The issue of copyright is introduced to children in primary six, through the school's Online Safety scheme.
- Lessons will be given in Online Safety and sensible use of the internet. These lessons will follow learning objectives set out in the school's Online Safety scheme to ensure progression.

2.4 – Online Safety and Staff

All staff will be introduced to the Online Safety Policy and its importance explained. Staff will be asked to read and sign the **Acceptable Use Policy for Staff (Appendix 2)** which focuses on Online 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 system.

Staff should only use their own personal mobile phone or digital device in **exceptional circumstances**. During working hours, all members of school staff should ensure their mobile phone is out of sight. School provided devices, such as teacher iPads or digital cameras, should be the only choice when taking photographs or videos of children. iPads have been provided to all teaching staff and no personal device should be used to photograph or video children **in any circumstance**. In addition to this, staff should not hold images of Glengormley Integrated Primary School children (with exception to their own children/family) on any personal device.

Staff have been given enhanced internet access and they must ensure that no child is given access to a computer that they are logged on to unless being supervised in a one to one situation. This means the child will not be able to access sites that may contain inappropriate material.

Staff should always ensure that any internet searches involving sites that they 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. The use of such sites (E.g. YouTube) should only take place after the content has been checked, therefore ensuring that children are not exposed to inappropriate content.

2.5 – Online Safety and Parents

The Online Safety Policy will be published on the school's website and parents will be encouraged to read the document. Glengormley Integrated Primary School will look to promote Online Safety awareness within the school community which may take the form of information evenings for parents/carers, information leaflets/publications through Seesaw and/or links on the school's social media platforms. Parents/carers of children in Foundation Stage and Key Stage One will be required to sign their child's **Acceptable Use Policy (Appendix 1a)**.

2.6 – Information System & Internet Security

Staff and children 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 will be made available to the school Principal and Online Safety Coordinator using Securus.

Connection of non C2K devices to the internet e.g. personal devices such as iPads and/or mobile phones through the controlled C2K Wireless network is subject to the same level of filtering as the main school system.

2.7 – Email Use

- C2k recommends that all staff and children 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.
- Children may only use approved email accounts on the school system. These can be accessed by children through their My Links portal on C2k MySchool.
- Children must immediately tell a teacher when using their C2K email address (if activated) if they receive an offensive or unexpected e-mail.
- Children must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Simplified Logons can be used in the Foundation Stage/Key Stage 1 classes; however, it is the responsibility of the teacher to ensure all children log on to their own user account;

2.8 – The Use of VLEs (Virtual Learning Environments)

A virtual learning environment or VLE is an online education platform. It is used as an extension of normal school lessons and contains many tools to help children learn their subjects.

Within Glengormley Integrated Primary School, teachers make use of Fronter, Google Classroom (Google Apps for Education) and Seesaw. These VLEs are used as means of collaboration between teachers, children and parents.

The level of security access set within these VLEs is at the discretion of the class teacher. Settings can be adapted to allow children to access only their own work or to access both their own and others' work. Viewing and reviewing others' work is an important aspect of online collaboration and peer assessment and it is important that children are aware of the responsibility such access brings.

The use of VLEs (especially Google Apps for Education) is a new approach to E-Learning in Glengormley Integrated Primary School and as such, its use will be continually reviewed to ensure the provision for Online Safety is high.

2.9 – Care, Responsibility and Dangers of the Internet

All users should always have an entitlement to safe internet access, however we must recognise the risks associated with the internet and associated technologies. The use of these new technologies can put young people at risk within and outside the school. Some of the dangers of internet use 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;
- cyberbullying;
- access to unsuitable video/internet games;
- an inability to evaluate the quality, accuracy and relevance of the 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. In Glengormley Integrated Primary School we understand the responsibility to educate our children in Online Safety issues. We aim to teach children 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.

3.0 – Management of System and Internet Access

Access to the internet is through a filtered service provided by C2K for all wired desktops and laptops (C2k Managed) and school iPads and wireless laptops (C2k Wireless). These services both ensure that the educational use of the school's digital resources is safe and secure, protecting users and systems from abuse.

Members of staff may have access to the internet through their own personal mobile phones or other technical devices with 3G/4G capabilities. The school has no ability to monitor or track the use of these devices however staff should adhere to the guidelines set out in the Staff Code of Conduct in relation to personal devices. If any member of staff is suspected of viewing or displaying illegal/inappropriate material on their own device, disciplinary procedures may be followed.

3.1 – Authorising Internet Access

- The school will maintain a current record of all staff and children who are granted internet access.
- All children must read and sign the **Acceptable Use Policy for Children (Appendix 1a/b)** every year. It will be explained to them by their teacher every year and a signed copy of each child's agreement will be held by the Online Safety Coordinator.
- All staff must read and sign the **Acceptable Use Policy for Staff (Appendix 2)** before using any school ICT equipment.
- All Parents of Foundation and Key Stage One children must read and sign the document **Acceptable Use Policy for Children (Appendix 1a)** before their child can be granted access to the use of any ICT equipment within the school.

3.2 – Assessing the Risks of Internet Access

- The school will take all reasonable precautions to ensure that users access only appropriate material. It is however, impossible to ensure that unsuitable material will never appear through the school's digital media.
- The Online Safety Team and the Principal will ensure that the Online Safety Policy is implemented and compliance with the policy is monitored.

3.3 – School Usernames and Passwords

3.3.1 – Teachers' Usernames and Passwords

- At no point should a teacher share their personal username or password with anyone, in order to safeguard their internet use and email security.
- Anyone found using a teacher's username and password that is not the owner of those details will be answerable to the Principal.
- If any member of staff suspects that their account has been accessed by another person, they must report it to the Online Safety Co-Ordinator at once.

3.3.2 – Children's Usernames and Passwords

- All children in Key Stage Two are expected to log on using their individual username and password.
- Any child found giving out or using another child's username and password will be dealt with by a member of the Online Safety Team and if necessary, the situation may be escalated to the School Principal.
- Teachers should not give generic passwords to all the children in their class. Children (who are not Simplified Log-on users) must be responsible for their own username and password and these must be individual to each child.

3.4 – Community Use of the Internet

- Any community use of the school internet through evening courses etc. must be treated as if it were children using the network and as such must sign an **Acceptable Use Policy for Children (Appendix 1b)**.

3.5 – Access to C2k Managed School Server

- Access to the school's C2k Managed server is monitored and granted by the school Principal. A record of the various levels of access granted to staff is recorded in the school's Register of Access. This document is updated, when required, by the school Principal.

4.0 – Communication of Online Safety Policy

4.1 – Introducing the Online Safety Policy to Children

- Rules for internet access will be posted in all rooms with access to the internet in school. Due to our wireless network, this must include all classrooms and the Portal (computer suite).
- Children will be informed that their internet use will be monitored.
- Online Safety lessons will be introduced at the beginning of each half-term to

raise the awareness and importance of safe and responsible internet use.

- These Online Safety lessons will follow the progression of the school's Online Safety scheme.

4.3 – Staff and the Online Safety Policy

- The Online Safety Policy will be distributed to staff by email and attention drawn towards it at the beginning of each school year or before policy review.
- Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

4.4 – Enlisting Parents' Support

- Parents' attention will be drawn to Online Safety policy through the school's website.
- Parents will be encouraged to discuss Online Safety with their children at specific points of the year, e.g. Internet Safety Week in February or following parental updates through Seesaw.

5.0 – Roles and Responsibilities

As Online Safety is an important aspect of Safeguarding and Child Protection within the school, the school's Safeguarding Team have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the Online Safety Co-ordinator to keep up-to-date with current Online Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The Safeguarding Team has the responsibility for leading and monitoring the implementation of Online Safety throughout the school however the Online Safety Coordinator should be the go-to for school staff regarding day-to-day issues.

The Safeguarding Team/Online Safety Co-ordinator have the responsibility to update Governors about Online Safety and all governors should understand the issues relevant to our school in relation to local and national guidelines and advice.

5.1 – Responsibilities: Online Safety Coordinator

Our Online Safety Coordinator is the person responsible to the Principal and the Board of Governors for the day-to-day issues relating to Online Safety.

The Online Safety Coordinator:

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents;
- leads curriculum development on Online Safety and supports the school's Digital Leader team in the promotion of safe and effective online behaviours;

- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident;
- provides training and advice for staff;
- liaises with the Education Authority;
- receives reports of Online Safety incidents and maintains a log of incidents to inform future Online Safety developments;
- reports to the Senior Leadership Team as required;
- receives appropriate training and support to fulfil their role effectively;
- has responsibility for informing C2K, and keeping a log in the Online Safety Log Book, of any occasions where inappropriate material has not been picked up by the school's filtering system.

5.2 – Responsibilities: Board of Governors:

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

5.3 – Responsibilities: The Principal:

- is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day-to-day responsibility for Online Safety is delegated to the Online Safety Co-ordinator;
- The Principal and the Vice Principal should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

5.4 – Responsibilities: Teaching and Support Staff must:

- have an up-to-date awareness of Online Safety matters and of the school's current Online Safety policy and practices;
- embed Online 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 **(Appendix 2)**;
- report any suspected misuse or Online Safety issues to the school's Online Safety Coordinator.

5.4.1 – Online Safety Skills Development for Staff

Online Safety training is an essential element of staff induction and should be part of on-going Continuous Professional Development programme. Through this Online 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 information and training on Online Safety issues through the Online Safety Coordinator at staff meetings and School Development Days;
- All staff must be made aware of individual responsibilities relating to the safeguarding of children within the context of Online 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 Online Safety into their activities and promote awareness within their lessons;
- All staff members will receive a copy of this Online Safety policy and Acceptable Use of the Internet Agreement. All staff must read and sign the Acceptable Use of the Internet Agreement;
- Teaching staff members who have been granted enhanced internet access (E.g. YouTube) will be informed of the appropriate use.

6.0 – The Safeguarding Team

The Safeguarding Team in Glengormley Integrated Primary School consists of:

Mr Nigel Arnold	Principal Designated Teacher
Ms Lyn Johnston	Deputy Designated Teacher School Governor Safeguarding and Child Protection Coordinator
Mrs Leanne McCord	Chairperson of Board of Governors
Mr Brendan Nellis	Designated Governor for Child Protection
Mr Mark Donaghy	Online Safety Coordinator School Governor

7.0 – Effective Handling of Online Safety Policy Breach

To deal with any incidents of technology misuse by children which arise, the school's Positive Behaviour Policy will be followed. Children must be made aware that the repeated misuse of the internet may lead to their access to it being denied. Child misuse will be dealt with by the Online Safety Coordinator. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed. Staff misuse will be dealt with by the Principal. Where the incident involves child abuse, the Designated Teacher for Child Protection and Safeguarding must be notified, and the school will follow procedures as set out in the school's Safeguarding and Child Protection policy.

Issues of internet misuse and access to any inappropriate material by any child should be reported immediately to the school's Online Safety Coordinator and recorded in the school's Online Safety log, giving details of the site and the time. In the case of a very serious incident, related to Safeguarding and Child Protection, a record of the incident will be kept in the locked Safeguarding and Child Protection cabinet in school, as per procedure.

Some Online Safety issues, such as harassment, trespassing in others' accounts, identity theft, physical and emotional harm or the possession of explicit or indecent images, may have legal consequences. For these purposes, it is essential that evidence of misuse is secured. This may be done on the C2K network using Securus but where this is not applicable, a suspect device must be secured by the Online Safety Coordinator or Principal and not be used or viewed until advice has been sought from the Education Authority and if necessary, the PSNI.

Following a major incident, a comprehensive debriefing will occur to review the school policy and procedures. Any changes to the school's policy, logs of misuse or changes to the school's filtering controls will be made available to the:

- Principal;
- Board of Governors;
- Safeguarding Team.

7.1 – 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 (Sexual Offences (NI) Order 2008); grooming, incitement, arrangement or facilitation of sexual acts against children (Protection of Children (NI) Order 1978);

- possession of indecent images (Section 62 of The Coroner's and Justice Act 2009); criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (Public Order (NI) Act 1987);

- 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;
- online 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 legal misuse. Incidents will be dealt with promptly and in a proportionate manner. Members of the school community will be informed that incidents have been dealt with. Incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

8.0 – Communicating with the Community beyond the School

Glengormley Integrated Primary School promotes and provides up-to-date information about the school and showcases other aspects of school life through the use of its website, Facebook page, Twitter page and Seesaw. In order to minimise risks of any images of children being used inappropriately, or personal staff profiles being viewed by children, the following steps should be taken:

8.1 – School Website

- Group photos are used where possible, with general labels/captions;
- Only photographs of children with parental/carer consent will appear on the school's online platforms;
- No photographs that identify individual children by name will appear on the website;
- The point of contact for the school will be the school telephone number, school address and the info@ school email address.

8.2 – Glengormley Integrated Primary School Public Facebook Page

- Group photos are used where possible, with general labels/captions;
- Only photographs of children with parental/carer consent will appear on the Facebook page;
- No photographs that identify individual children by name will appear on the Facebook page;
- The purpose of this Facebook page is primarily for publicity. Questions from parents are discouraged and staff should not reply to any questions asked. Parents will be directed to Seesaw or the School Office if they wish to make an enquiry.
- The school's public Facebook page is managed by Mrs Coburn.

8.3 – Glengormley Integrated Primary School Twitter Page

- Group photos are used where possible, with general labels/captions;
- Only photographs of children with parental/carer consent will appear on the Twitter page;
- No photographs that identify individual children by name will appear on the Facebook page;
- The purpose of the school's Twitter page is primarily for publicity – it is an extension of the Facebook page and automatically reposts any information on the Facebook page. Questions from parents are discouraged and staff should not reply to any questions asked. Parents will be directed to Seesaw or the School Office if they wish to make an enquiry.

8.4 – Seesaw

- Information is provided to parents/carers through both the Announcements feature and through uploaded copies of school notes.
- Individual class teachers are responsible for monitoring their own class's Seesaw account and updating parents/carers with appropriate information.
- Teachers should endeavour to reply to parents'/carers' questions during normal working hours and should, where possible, avoid contact outside these times.

9.0 – Social Networking

This is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs.

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. Children will not be allowed to use any social software which has not been approved by teaching staff and the C2K filtering service. Teaching staff will have access to social media through their enhanced user profile. This access must be carefully and responsibly moderated.

In line with good Safeguarding and Child Protection practice, staff are advised that:

- It is not acceptable and is against school policy for staff to be friends or follow school children on social networking sites;
- It is not acceptable and is against school policy for staff to be friends or follow ex-school children on social networking sites, unless there is a prior relationship with said child/children outside the school environment.

In line with good Safeguarding and Child Protection practice, children and parents are advised that:

- It is not acceptable for children to request to be friends with a member of staff on a social network site. If a child requests to be friends with a member of staff on a social network site, the member of staff is required to inform their parent. If the member of staff is not the child's teacher, they should inform the child's teacher who will inform the child's parent.
- The use of social network spaces outside school is inappropriate for primary aged children. It is accepted, however, that some children will still use them. Children's disclosure to social networking spaces must be closely monitored to ensure they are only exposed to age appropriate content.
- Children should set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

10.0 – 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, Glengormley Integrated Primary School has a specific policy on the acceptable use of mobile phones and related technologies.

The use of mobile phones by children is strictly prohibited on the school premises. Children will be informed that they do not need to have a mobile in school as any messages can be forwarded through the school office. In exceptional cases where a child in P5-7 may need to be contacted after school for the purposes of walking home/arranging transport, the class teacher should be made aware, in writing, that the child will have one in their bag. Phones must remain off and in the child's schoolbag whilst on the school premises. No child in P1-4 should have a phone.

Should staff become aware that a mobile phone is turned on, not in a child's school bag or has been used in school, it will be confiscated and locked in the school safe in the Principal's office. The mobile phone will only be returned directly to a parent/guardian. This policy also applies to Glengormley Integrated Primary School's extended schools provision.

Staff members should refrain from using their mobile phones or similar technology when in contact with children unless prior permission has been given. Staff accessing the internet in school on their own mobile phones must adhere to the expectations set out in **section 3.0.**

11.0 – Cyberbullying

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

Cyberbullying 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.

A record will be kept of all incidents of Cyberbullying in the schools Online Safety log. This allows the school's Safeguarding Team to monitor the effectiveness of the school's preventative strategies, and to review and ensure consistency in their investigations, support and sanctions.

Appendix 1a: Foundation & KS1 Children ICT Acceptable Use Policy

When using the ICT equipment in school these are the rules I will keep.

1. I will take good care of any equipment I use.
2. I will not eat or drink when I am using ICT equipment.
3. I will make sure my hands are clean before I use the equipment.
4. I will never leave an iPad or laptop lying around and I will tell the teacher when I am finished with it.
5. I will make sure the case is always on the iPad.
6. I will only use ICT equipment for what my teacher asks me to do.
7. I know that my teacher will look at what I have done in ICT time.
8. I will only take photographs of people if they say it's okay.
9. I will only use the camera or the microphone when my teacher tells me to.
10. I will remember that our computer equipment is for learning and must be shared.

I think these rules are important and I promise to stick to these rules to keep me safe and protect our ICT equipment.

Child's name and class ____________________________

I have discussed these rules with my child.

Parent Signature ____________________________

Parent/Guardian

Please discuss the ICT equipment rules with your child and return the slip signed. It is important the slip is returned to school as soon as possible.

Talk to your child about the importance of following these rules when using all ICT equipment (computers, laptops, iPads, interactive whiteboards etc.) at G.I.P.S. just like we follow our Golden Rules in school. Talk to your child about general safety when working on the internet, the importance of not giving out personal information to anyone and being respectful to the views and opinions of others online. Talk about what to do if they have any concerns about something they see on the internet/computer at home or in school. We will also be discussing these rules and their importance in our Online Safety lessons in class time.

Parent/Guardian

Please discuss the ICT equipment rules with your child and return the slip signed. It is important the slip is returned to school as soon as possible.

Talk to your child about the importance of following these rules when using all ICT equipment (computers, laptops, iPads, interactive whiteboards etc.) at G.I.P.S. just like we follow our Golden Rules in school. Talk to your child about general safety when working on the internet, the importance of not giving out personal information to anyone and being respectful to the views and opinions of others online. Talk about what to do if they have any concerns about something they see on the internet/computer at home or in school. We will also be discussing these rules and their importance in our Online Safety lessons in class time.

Appendix 1b: KS2 Children ICT Acceptable Use Policy

Responsibilities when using ICT Equipment

Children are responsible for good behaviour when using computers, laptops, iPads and any device which accesses the internet at Glengormley Integrated Primary School, just as they are in a classroom or a school corridor. General school rules apply.

Digital technologies (computers, laptops, iPads etc.) are provided for children to carry out work, conduct research and communicate with others. Access is a privilege, not a right, and that access requires responsibility. The following are not permitted:

1. Sending or displaying offensive messages or pictures;
2. Using bad or inappropriate language;
3. Harassing, insulting or attacking others;
4. Copying someone's work and pretending it is your own;
5. Using others' passwords or pretending to be someone else;
6. Trespassing in others' folders, work or files;
7. Deliberately wasting limited resources;
8. Destruction of technology through careless or deliberate means.

Online Safety

- Do not give any password or login name you have been given to anyone;
- Do not give out your own or anyone else's personal details including addresses, telephone numbers or email to any person, under any circumstances;
- Be polite and appreciate that other users might have different views to your own;
- Report any concerns regarding on-line activity to your teacher immediately.

Consequences

1. Breaking or not following the above rules may result in a temporary or permanent ban on use of technology and internet access.
2. Parents will be informed about the misuse.
3. Additional disciplinary action will be taken in line with existing school rules as appropriate to language or behaviour.

I have read and understand the above and agree to use computers, laptops, iPads and any devices which access the internet within these guidelines.

Child's Name: ____

Child's Signature: ____

Date: ____

Appendix 2: Staff (and Volunteer) ICT Acceptable Use Policy Agreement

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 access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for child learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that children receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school. Staff can access the school system whilst outside the school environment via the C2K My School App and as such, this access should only occur on a private system.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using the school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- 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 digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school's website/VLE/Facebook Group) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with children and parents / carers using official school systems. Any such communication will be professional in tone and manner. **(See Staff Code of Conduct).**
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and C2K have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school's ICT facilities:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless it is cleared by C2K and carried out by the school's C2K manager;
- I will not disable or cause any damage to school equipment, or the equipment belonging to others;
- I understand that data protection policy requires that any staff child data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not download or distribute copies (including music and videos);

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school;

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Education Authority and in the event of illegal activities the involvement of the PSNI.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: ....

Signed: ....

Date: ....

Appendix 3: iPad Acceptable Use Policy for Staff

This policy is linked to the following school policies:

Online Safety Policy
ICT Policy
Safeguarding and Child Protection Policy

This policy operates in conjunction with the Online Safety Policy and is designed to help and protect staff in Glengormley Integrated Primary School. It is not permissible to use personal iPads or other hand-held devices (i.e. devices which have not been provided by the school) for learning and teaching purposes, in the classroom or for any school-based activity. When using an iPad, supplied by the school, you are agreeing to and accepting that:

Administration and Security

- The iPad is the property of the school;
- Use of the iPad is for educational purposes and all relevant school policies are applicable, including the *Computer and Internet Acceptable Use Policy*;
- The device is for your use only outside school, and must not be lent to any other party, including children of the school, family members etc;
- The device can be recalled, by the school, at any time;
- iPads should be brought to school each day in a fully charged condition;
- Every precaution is taken to avoid damage to or loss of the devices;
- The case provided by the school must be used;
- The iPad and charger must be stored in a secure place, which is out of sight, when not in use;
- A four-digit security PIN must be used to secure the device and the auto-lock is set to two minutes.
- The security PIN of the device is held only by teachers and is the same four-digit code on all staff devices;

Data Storage and Use

- Files stored on the iPad will not be regarded as private. The school reserves the right to monitor, review and examine the content, internet history, usage, communications and files of users, and, where it deems it to be necessary, will intercept and delete material which it considers inappropriate, and prohibit the use of such material;
- Documents on the iPad should be backed-up regularly using the Cloud Storage capabilities (Google Drive);
- Personal Apps and music (through personal Apple iTunes accounts) which are deemed suitable by the teacher for educational purposes and relevant to agreed learning and teaching programmes can be installed. Teachers must take care when purchasing apps/music, or any paid content for their personal use, that they are signed in to their own Apple iTunes account and not the school's account. The school's account must be reimbursed for any personal paid content bought mistakenly;
- Apps installed via school/key stage iTunes account must be for educational purposes and relevant to agreed learning and teaching programmes;
- Personal e-mail accounts must not be installed through the Mail App or any other

third-party App (Hotmail, Gmail etc.) but personal email can still be accessed through Safari or other browsers if the 'save password' option is not engaged;

- Other personal items, such as documents, audio, text, photographs, videos - must NOT be stored on this device.

Use of Digital Media

- The use of the camera must be in line with the school's *Online Safety Policy* and the *Safeguarding and Child Protection Policy*. Individual photographs of children should not be taken;
- I am responsible for understanding and adhering to all copyright requirements and policies related to digital media and the use of this iPad.

Professional Development

- Undertake professional development e.g. attend training sessions; collaborate with colleagues in the development of best practice and resources;
- Attend and contribute to year group/key stage support sessions;
- The school expects and requires all users to comply with the standards outlined in this policy and to follow its protocols.

Reporting Incidents

- In the case of loss, theft or other damage occurring outside of school, the ICT coordinator must be informed as soon as possible. In consultation with the ICT coordinator, it is the responsibility of the teacher to follow school procedures in the event of the iPad needing repair or replacement.

I understand and will abide by this Acceptable Use Policy. I further understand that should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.

This policy is subject to change.

Signed : ....

Date : ....

Appendix 4: Classroom Rules for Computer and Internet Use

GLENGORMLEY INTEGRATED PRIMARY SCHOOL

Rules for Computer and Internet Use

- Ask permission before using the Internet.
- Only use your own network login and password.
- Do not bring software or disks into school without permission.
- Do not ignore pop up boxes you do not understand – tell a teacher if you see something you think you shouldn't have.
- Only e-mail or contact people you know or people your teacher has approved.
- Messages you send must be polite and sensible. Emails containing offensive language will be filtered and blocked. However, it is your responsibility to ensure everything you send is appropriate.
- Do not open e-mails/attachments from someone you do not know. Inform a teacher.
- You must never give out personal details; home address, telephone number.
- If you see anything you are unhappy with or receive messages you do not like, turn your monitor off and tell a teacher immediately.
- You must not search for offensive material.
- The school may check your computer files and Internet sites you visit.
- Deliberately breaking these rules may result in you not being allowed to use the Internet or computers.