Grange Park Primary School
E-Safety Policy

Version	Date Published	Date To Be Reviewed	Date on website (if applicable)
1.0	March 2018	January 2019	March 2018

Contents

1. Context and Rationale

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 and information technologies are powerful tools, which open up new opportunities for everyone. With these opportunities we also have to recognise the risks associated with the Internet and related technologies.

Grange Park Primary School has a range of ways for pupils and teachers to access the Internet, including PCs in classrooms, ICT suite and over 150 iPads. The use of these exciting and innovative tools in school 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.

"All schools should have their own E-Safety Policy, which must operate in conjunction with other school policies including Behaviour, Child Protection, Anti-Bullying and Acceptable Use. E-Safety must be built into the delivery of the curriculum. ICT is a compulsory cross-curricular element of the revised curriculum and schools must ensure acquisition and development by pupils of these skills"
DENI E-Safety Guidance, Circular number 2013/25

It is the responsibility of the school's staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. E-Safety covers not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The School must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The E-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope of Policy

This policy applies to all members of the Grange Park Primary School community who have access to and are users of the school ICT systems, both in and out of the School. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure E-Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to E-Safety incidents that occur outside school hours, the School will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. E-Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any

member of the School community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward.

The school's E-safety policy operates in conjunction with other policies including those for Behaviour Management, Bullying, Data Protection and Child Protection.

The policy has been agreed and approved by ICT Coordinator, Senior Leadership Team, Designated Child Protection Officer and Board of Governors. It will be reviewed annually and will be linked to the review of any other policy mentioned above.

3. Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which pupils need to be reasonably protected. At an appropriate age and maturity they will need to learn to recognise and avoid these risks — to become "Internet-wise" and ultimately good "digital citizens". Schools need to perform risk assessments on the technologies within their school to ensure that they are fully aware of and can mitigate against the potential risks involved with their use. Pupils need to know how to cope if they come across inappropriate material or situations online. The school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.
DENI E-Safety Guidance, Circular number 2013/25

The main areas of risk for the School can be categorised as the Content, Contact and Conduct of activity.

1. Content
   - Access to illegal, harmful or inappropriate images or other content.
   - Access to unsuitable video / internet games.
   - An inability to evaluate the quality, accuracy and relevance of information on the Internet.

2. Contact
   - Inappropriate communication / contact with others, including strangers.
   - The risk of being subject to grooming by those with whom they may make contact on the Internet.
   - Cyber-bullying.
   - Unauthorised access to / loss of / sharing of personal information.

3. Conduct
   - The potential for excessive use which may impact on the social and emotional development and learning of the young person.
   - Plagiarism and copyright infringement
   - Illegal downloading of music or video files

- The sharing/ distribution of personal images without an individual's consent or knowledge.

Many of these risks reflect situations in the offline world and it is essential that, as already mentioned this E-Safety policy is used in conjunction with other School policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them appropriately.

In Grange Park P.S. we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach pupils appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies in and beyond the context of the classroom.

4. Roles and Responsibilities

As E-Safety is an important aspect of Child Protection within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. They are supported in this by all stakeholders in the school community.

4.1 Governors will:

- Consult with the Principal and ICT Coordinator and other relevant adults to approve the E-safety policy and continue to review its effectiveness.
- Receive regular information about E-safety incidents and monitoring reports of ongoing issues if necessary.
- Participate in school's training/ information sessions for staff and parents.
- Appoint an E-safety Governor who will support and liaise with the Principal and ICT Coordinator on E-safety issues arising.

4.2 Principal (with the support of SLT) will:

- Liaise with the ICT Coordinator and Board of Governors and Child Protection Team regarding E-safety matters.
- Deal with any serious e-safety allegations being made against a member of staff.
- Ensure the ICT Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues as relevant.

4.3 Designated Child Protection Officer/ Deputy Designated Child Protection Officer will:

- Be trained in e-safety issues and be aware of potential for serious child protection issues to arise from sharing of personal data, access to illegal/inappropriate materials,

inappropriate online communication with adults/strangers, potential or actual incidents of grooming and cyber bullying.

4.4 ICT Coordinator

By taking on the role of the e-safety coordinator the ICT Coordinator takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school's policies/documents.

The ICT Coordinator will also:

- Ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.
- Provide training and advice for staff
- Liaise with the ELB and DENI on E-Safety developments
- Liaise with C2K and iTeach to ensure e-safety measures as recommended by DENI are in place on their networks in the school.
- Receive reports of E-Safety incidents and create a log of incidents to inform future E-Safety developments
- Attend relevant meetings with Board of Governors to discuss current issues
- Review incident logs
- Monitor and report to Principal any risks to staff of which the E-Safety coordinator is aware.
- Ensure that the school infrastructure and individual workstations are protected with up to date virus software. (Through implementation of C2K advice and iTeach technical support.)
- Ensure that any software or apps purchased outside of C2K allocation are checked regularly to reconcile the number of licences purchased against the number of software installations.

4.5 Teaching and Support Staff will:

- Have an up to date awareness of e-safety matters and of the current school E-safety policy and practices.
- Read, understand and sign the schools Acceptable Use Policy.
- Report any suspected misuse or problems to the ICT Coordinator.
- Only communicate on a professional level on the official school systems either C2K or the schools Gmail accounts. Emails should be sent in accordance with the School's guidance.
- Embed e-safety into all aspects of the curriculum.
- Monitor ICT activity in lessons and extra-curricular activities.
- Be aware of e-safety issues related to the use of mobile phones, camera and hand held devices and implement the current school policy with regard to these devices.
- Undertake all e-safety training as organised by the school.

4.6 Pupil Digital Leaders will:

- Inform the ICT Coordinator of potential issues regarding e-safety

- Present information during an assembly on Safer Internet Day

4.7 Pupils will:

- Read, understand, sign and adhere to the schools Pupil Acceptable Use Policy
- Report abuse, misuse or access to inappropriate materials to the ICT Coordinator, Principal or another staff member they trust.
- Be introduced to email and taught about the safety and 'netiquette' of using email both in school and at home.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school if it affects their membership or another member of the school community.

5. E-safety Education

Grange Park Primary School recognises that in a rapidly evolving online world e-safety education needs to regularly revisited to explore up to date risks and responsibilities. With this in mind E-safety education is essential for all stakeholders in the school community.

5.1 E-safety Education for Staff

- All staff will receive regular information and training when necessary on e-Safety issues through the ICT Co-ordinator at staff meetings or via email.

- All staff will 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.
- New staff members will receive a copy of the e-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.
- All staff are encouraged to incorporate e-Safety into their ICT activities and promote awareness within their lessons. (ICT Team will share resources when appropriate with teachers.)
- All staff will be made aware of their responsibility to minimise risk of using the Internet by restricting lessons incorporating ICT to specific learning outcomes and guiding pupils towards appropriate online materials to meet these outcomes.

5.2 E-safety Education for Pupils

- A planned e-safety programme will be delivered as part of ICT / PDMU and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Child Exploitation and Online Protection (CEOP) resources will be used as a teaching tool and PSNI may be invited to the school to speak to KS2 pupils.

- Where appropriate, pupils will be taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet.
- Pupils will be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school.
- Pupils should be made aware that independent electronic research requires specific teacher permission and supervision and must be carried out in designated curricular areas only.
- Where pupils are allowed to search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit by providing specific, age appropriate guidance about words to use in a search engine or specific sites to explore that meet the lessons learning outcomes.
- Pupils will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be informed that all network and Internet use is monitored and that there will be strict consequences for its deliberate misuse.
- Pupils will be made aware that whilst the use of ICT technologies is a requirement of the Northern Ireland Curriculum, access to the Internet remains a privilege and it will be withdrawn if they fail to maintain acceptable standards of use.

5.3 E-safety Education for Parents and Carers

Parents and carers have an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. The school recognises that some parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will seek to provide information and awareness to parents and carers through:

- A section of the school website to promote e-safety.
- The publication of the E-safety policy either through Seesaw or the school website.
- Delivering E-Safety Guidance at key parent meetings and through social media.
- A designated E-Safety Parents' Event
- The annual requirement to read the Acceptable Use Agreement for pupils and sign the agreement following a discussion with their child.

6. Current Practice

6.1 Infrastructure and Networks

- Rules for digital technology use will be displayed in computer area and age appropriate versions will be displayed and referred to in all classrooms.
- Internet access for pupils is located in the classrooms and ICT room. All computers are in full view of people circulating in these areas. All iPads are used in open classroom areas again in full view of people circulating.
- Internet access is through 2 filtered services – one provided by C2k (for laptops and computers) and one by iTeach (for iPads).

6.2 Filtering

Both the C2K service and the iTeach service (Classnet) are filtered to prevent users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so because the content on the web changes dynamically and new technologies are constantly being developed. The responsibility for the management of the school's filtering policy is held by Principal and ICT Coordinator.

The Principal and ICT Coordinator manage the school filtering by:

- Monitoring reports of the use of C2k / Classnet which are available on request.
- Reporting breaches of the filtering systems to relevant service provider and keeping a record of these incidences.

Staff and pupils have a responsibility to:

- Report immediately to Principal and ICT Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- Avoid the use of any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

6.3 Communication

Like any business, Grange Park Primary School sees email as a valuable tool for communication and encourages staff to use it daily. We also encourage the use of email to communicate with parents.

- The school uses two official email systems '@c2kni.net' and '@grangeparkps.org'. Emails from these may be regarded as safe and secure. Email communications with parents, colleagues or contacts in a professional context should only be conducted through these two systems. Personal email addresses should not be used. Similarly, school accounts should not be used for personal correspondence.
- Email messages sent through these two systems will be analysed and filtered. Messages considered inappropriate will be held and either returned to sender or reported to the C2K/ System Manager.
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Spam or junk messages should not be opened or responded to and should be deleted.
- Any digital communication between staff and pupils or parents/carers by email, VLE and official school social media accounts must be professional in tone and content.
- Staff should not engage in correspondence with a pupil through the pupil's personal email account. If a pupil does contact a member of staff through email, the parent should be notified, a copy of the email forwarded to Principal and then the pupil should be encouraged to connect with the teacher through their parent's email account.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- The Principal and ICT Coordinator can deactivate email accounts in cases of misuse.

6.4 Browsing/ Using Search Engines

As mentioned above our school does offer protection with the supervision of children and a filtering software system is installed but this software is not always fool proof. Neither the school, nor C2K/iTeach can accept liability for materials accessed or any consequence of Internet access. We must therefore alert children to the risks they might encounter and educate them to make a safe and appropriate response whether this is in school or at home. Pupils using search engines are expected to not deliberately seek out offensive materials. Should any pupil encounter such material accidentally, they should report it to a teacher immediately.

Teachers registering on a website for school purposes should use school details such as address and phone number. Pupils should not register on websites during learning activities without prior consent from their teacher and again, school details should be used.

Access to any websites should clearly enhance pupils learning experiences.

When using the Internet at Grange Park Primary School, all users must comply with all copyright, libel, fraud, and discrimination and obscenity laws. Children should also be aware that not all information on the Internet is correct and therefore they should be encouraged to consider the author, date it was published and the content of information found. Like books, information found on the Internet must not be plagiarized, therefore children should be taught to follow general rules of referencing when including information sourced on the Internet.

6.5 Teaching in a Virtual Classroom

From time to time, teachers may use Virtual Classroom activities such as video conferencing and Learning NI to enhance their lessons. This allows teachers and pupils to collaborate with others both locally and internationally. Guests, teachers and pupils must agree to protocols before a session occurs. Parents and carers should also agree for their child to take part in video conferencing. Guests must only be invited to attend by teachers who will set up a meeting at a given time. Access to this conference is through an email which allocates a unique user name and password for one meeting which expires at the end of the session. Webcams will be switched off at all times except during conferences. The teacher must always be present during a conference. Only teachers will initiate, make or answer video conferencing calls.

6.6 Social Networking

At present, the school endeavours to deny access to social networking sites to pupils during school hours. The Principal uses a school Twitter account to publicise the school and connect with parents, all posts maintain the anonymity of pupils and are confined to general school news.

Staff may use Twitter / You Tube / VLE to enhance their lessons but should adhere to the following guidelines:

- Social Networking should only be included in lessons where it will clearly enhance the learning outcomes. E.g. connecting with the author of a class novel via twitter.
- In such cases as above, approval must be granted by the Principal who will facilitate the lesson through the school Twitter account.

- Any comments pupils wish to post should be approved by their teacher and remain professional and polite in tone and content.
- Children should remain anonymous in any online posts. (No names or personal details.)
- Teachers should watch any YouTube (or similar) videos fully before including them in their lesson to ensure all the content is appropriate and educationally beneficial. If a video contains an advertisement, the screen should be blanked and the sound turned off until it has finished.
- Teachers should review the privacy settings of any VLE to ensure they are set to the adequate level for planned activities.
- Teachers and pupils should report any incidents of inappropriate content, privacy violation or cyber bullying as a result of social networking immediately to the school Principal and ICT Coordinator.

The school also recognises that staff (teaching and non-teaching) may use social networking sites outside of school in their private life. Whilst the school does not have the jurisdiction to control this, they do still have authority in safe guarding the privacy of pupils and the public image of the school and therefore request that staff keep clear boundaries between their professional and private lives online. If a staff member's out of work online activity causes potential embarrassment for the school or detrimentally affects the school's reputation, then the Board of Governors is entitled to take disciplinary action.

If staff choose to use social media for private purposes, they are encouraged to adhere to the following guidelines for their own online protection:

- Privacy settings on any online profiles should be set to maximum privacy and deny access to unknown individuals without a request first.
- Grange Park Primary School should not be linked to any online activity from private accounts. (Online activity should not link the staff member to the school either directly by name or through 'anecdotes' of their working life.)
- Staff will not add pupils, past and present, as 'friends'. If a pupil tries to add a teacher, they should reject the request, make the Principal aware of the request and notify the child's parent. Likewise, staff should not seek out pupils, past or present and 'request friendships.'
- If a member of staff is the recipient of defamatory comments about them on Social Networking sites, made by children, parents or other stakeholders, the Principal should be informed immediately and contact made to the relevant services.

Pupils and parents will be advised that the use of social network spaces outside of school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them. They will be advised to never give out personal details of any kind or upload personal photographs, which may identify them or their location. Pupils will also be advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. Pupils and parents are asked to report any incidents of cyber bullying to the school.

6.7 Personal Devices

Pupils Use of Personal Devices

Grange Park Primary School is very well equipped in ICT resources and therefore does not permit pupils to bring their own devices such as tablets or laptops into school.

Mobile Phones

The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety and therefore the following guidelines must be adhered to:

- The school takes no responsibility for mobile phones. Mobile phones are brought to school entirely at the owners own risk.
- Mobile phones must be switched off and out of sight during school hours- whilst the pupil is in class, on the school grounds or on school related off site activities.
- Phones must never be used to photograph staff or other children.
- If a pupil is found to be using a mobile phone or device during the school day then it will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers by the Principal.
- If a pupil uses a phone inappropriately, this will be regarded as a serious offence and the Principal will decide on the appropriate action to take in line with the school's discipline policy.
- It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. The Principal and SLT may consider it appropriate to refer any such matter to the PSNI.
- If images (photographic or video) of other pupils or staff have been taken, the phone will not be returned to the pupil until the pupil, in the presence the Principal and in most cases the pupil's parent/carer, has removed the images. The Principal will always contact the pupil's parent/ carer before asking the pupil to delete material from their mobile phone.
- The Principal will contact the parent/carer in all cases where inappropriate photographs/videos/audio files have been found and if necessary, the PSNI may be contacted.
- Should parents need to contact pupils during the school day, or vice-versa, this should be done following the usual school procedure: via the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Wearable Technology

Grange Park Primary School has taken the decision to ban wearable technology for pupils e.g. Apple watches. These items can be used as communication devices and cause greater distraction than mobile phones. If a child is found to have wearable technology, then this will be treated in the same manner as using a mobile phone.

Staff Use of Personal Devices

All members of teaching staff have been resourced with a school owned iPad, laptop and each year group has a digital camera to share. This means that we do not require teachers to use

personal electronic devices during school hours for work purposes. Staff may bring personal devices onto the school site and may use them in their free time outside of timetabled school hours. E.g. Lunch time. They must not however connect into the school Wi-Fi system for personal use. (Either C2K or iTeach)If a member of staff feels they have reasonable grounds for using a particular personal device in a lesson for substantial educational benefits to their pupils they may discuss this with the Principal.

Mobile Phones

Grange Park Primary School recognises that staff and volunteers may want to bring a mobile phone to their place of work. Staff use of mobile phones, only when necessary, should be discreet. The following guidelines should also be adhered to for staff's own protection and to safeguard the pupils:

- The school takes no responsibility for staff or volunteer's mobile phones. Mobile phones are brought to school entirely at the owners own risk.
- Mobile phones should not be used in the classroom setting and should not be visible to pupils throughout the school. Phones brought into the classroom setting must be either switched off or set to silent.
- Staff may use their phones during non-directed time (before school, lunch time and after school) but not in the presence of pupils.
- Should a member of staff need to be reached the most effective method is through calling the school office.
- Staff should not use a mobile phone to record images (photographic or video) of pupils – a school owned device should be used.
- On occasions where a group of pupils may go off site with their teacher, the Principal may request that the teacher uses their mobile phone during the trip to take and email images (photograph or video) for social media (twitter). In such cases, a minimal amount of images should be taken and, after the trip is finished the staff member must delete the images from their device in the presence of another teaching staff member.
- If a staff member is found to be using a phone inappropriately, this will be regarded as a serious offence and the Principal will decide on the appropriate action to take in line with the school's staff discipline policy, this may result in action also being taken by the Board of Governors and external agencies such as PSNI being informed.

Wearable Technology

Staff use wearable technology in school entirely at their own risk. The school takes no responsibility for such devices. Similar to mobile phones we ask that staff activate a 'Do not disturb' or 'Flight mode' during directed time to ensure they are not distracted from teaching by message or call alerts.

Parents and Visitors Use of Personal Devices

Parents and Visitors are made aware of the following guidelines and we appreciate their support in adhering to these in order to keep our pupils safe:

- Mobile phones should not be used in the classroom setting and only discreetly in the school building.
- Mobile phones should not be used to take photographs within the school ground unless permission has been granted by the Principal e.g. for a specific event such as the nativity or to record necessary maintenance etc.
- Photographs that parents take of pupils on school grounds are for personal family use only and should not be posted on public social media without prior permission from the Principal. Similarly, photographs sent home to parents via Seesaw are for personal family use only and should not be posted on public social media.

6.8 Digital Photographs and Videos

At Grange Park Primary School, we take photographs and videos for a variety of reasons:

- To record activities and events for posterity to the school
- As a personal record for parents (shared through Seesaw and school website.)
- To record and evidence groups' and individuals' work and achievements
- To publicise the school and its achievements in the wider community (shared through website, twitter and local press)

Photographs and video clips will only be taken of those pupils for whom permission has been received from Parents/Carers. All new pupils should complete this permission slip on enrolment to the school. If a parent/ carer does not wish their child to be photographed their wishes will be respected. An effort will be made to ensure that any images of pupils used beyond the school community will not lead to a child being identified or personal information being disclosed.

6.9 School Website

The Grange Park Primary School website (www.grangeparkps.org) and social media pages (Twitter) promote and provide up to date information about the school, as well as giving pupils an opportunity to showcase their work and 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.
- Pupils' photographs or work are not named.
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

6.10 Password Security

Staff

Password security is essential for staff, particularly as they are able to access and use student data. All staff are provided with an individual login username and password for use on the C2K system and are required to set their own lock code on their staff iPad. The following guidelines must also be adhered to:

- Staff must have secure passwords and must not share these with anyone.
- Staff users must make sure that workstations are locked or logged out when unattended in the classroom.
- Staff users must not leave their iPad unlocked and unattended. If an iPad is left in a classroom unattended e.g. over lunchtime it should not be left in an area accessed by pupils and should preferably be left out of sight e.g. in a drawer or store.
- Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.

Pupils

All pupils in Grange Park Primary School will be allocated a user name by C2k and as part of the e-safety programme will be taught the importance of confidentiality and the responsibility of security when accessing a shared network.

Pupils in Primary 1-3 will login as a foundation user with a basic username and password or as a class user. Pupils in Primary 4-7 will login with their C2k username and a password agreed with the class teacher. The class teacher can reset any pupil's password or unlock their account if necessary. The ICT Coordinator, as System Administrator, can access or lock any account to investigate or prevent access in the event of misuse.

The following guidelines (covered in the pupils Acceptable Use Agreement) must also be adhered to:

- Pupils must use only their own network username and password.
- Pupils must not share their username and password. If they are written down they must be kept safe.
- Pupils are not allowed to deliberately access files on the school network that belong to their peers, teachers or others.
- Shared accounts e.g. Google Drive or Scratch are for school use only, whilst pupils know the login details they must not access these without their teacher's permission. Pupils must not share these account details outside of school.

If a pupil chooses not to follow these guidelines their account may be suspended and access to computers/iPads restricted. If this problem continues the matter will be reported to the School Principal and further action will be taken as deemed appropriate.

6.11 Cyber Bullying

As mentioned above, cyber bullying misuses technology and whilst teaching and learning will highlight appropriate use and responsibilities the risk cannot be completely eliminated. Any member of the school community could be a victim. Online bullying or harassment is the same as bullying or harassment in person and is unacceptable in all circumstances. Any incidents will be dealt with in line with the school's Discipline Policy

All users should report incidents to the Principal, Designated Officer for Child Protection or the ICT Coordinator as soon as they occur. If the incident involves a pupil the parents/carers will be contacted and outside agencies (such as PSNI) may be involved.

Pupils and staff will be reminded regularly of good practices and responsibilities. Posters reminding users to report incidents will be clearly visible in all ICT areas.

6.12 Data Protection

At times, staff may need to access parts of the network (SIMS) that contain personal data or work with confidential online data pertinent to pupils' progress. In these instances, staff have a responsibility to ensure its safety by using secure password protected computers which are properly 'logged off' at the end of each session.

If staff need to download this data, any memory stick should be kept securely and the data deleted from the device once its use is complete. Staff are discouraged from printing this data for personal use and if on occasion it is printed, the document should be shredded after its use is complete.

7. Managing Incidents

7.1 Actions and Sanctions

As mentioned in the sections above any e-safety incident should be reported to the ICT Coordinator and Principal. Investigation and sanctions will be in line with the Acceptable Use Policy and school's Discipline Policy.

Further to this, should technology or online platforms be used as a means by which to bully another, incidents will be dealt with in line with the schools' Anti Bullying Policy.

7.2 Handling of E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and the ICT Coordinator informed.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions within the school discipline policy may include – interview with the class teacher/ Principal, informing parents/carers, removal of Internet or computer access for a period. Sanctions will be in measured response to the incident and persistence of the problem.

8. Policy Review

This policy will be kept under review. It will be modified if necessary to meet changes in the curriculum. The overall ICT programme for the school will be evaluated at staff meetings, both formal and informal and if problems are identified appropriate action will be taken.

To be reviewed Jan 2019

Addendum

- Network administrators reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibly – they will respect the right to privacy whenever possible.

- Any parent or member of staff who wishes to discuss this document can put any questions to: -

Ms A White (Principal)
Or
Miss C McCartney (ICT Co-ordinator)

Grange Park Primary School

Three Way Agreement for Safe, Effective and Acceptable Use of Internet and Digital Technologies/ E-safety

Pupils

The school computers and iPads are connected to the Internet to help our learning. These rules help us to be fair to others and keep everyone safe.

General Rules

- I am responsible for my own behaviour, just as I am anywhere else in school. I will follow my class and the school rules.
- I will respect hardware and software available to me.
- I will respect the work of others.
- I will use only my own username and password to log in, which is a secret.
- I will only use the computers and iPads for schoolwork and home learning unless permission has been granted.
- Personal printing is not allowed on the school network for cost reasons.
- I understand that I must never give out my name, home address, phone number, school name, address, phone number or email address or arrange to meet someone.
- I understand I must not give out my friend's personal information.
- I will only look at or delete my own files.
- I will not access other people's files unless permission has been given.
- I will not bring in media or storage devices from home unless permission has been given.
- I will not play games unless specifically assigned by the teacher.
- I will get a teacher or parent/carer to check the content if I create my own website.
- If I need help I know who to ask.
- If I see anything on the Internet or in an email that makes me feel uncomfortable, unhappy or something I do not like, I will tell a teacher immediately. I understand that my report would be confidential and would help protect other pupils and myself.
- I know I can go to thinkyouknow.co.uk for help.

Internet Use

- I will ask permission from my teacher before using The Internet and will only access services I have been given permission to use.
- I will use the Internet to help me learn and I will learn how to use the Internet safely and responsibly.
- I will not deliberately seek out offensive materials. Should any appear accidentally I will report it to a teacher immediately.
- I understand that the school may check my computer files and the Internet sites I visit.

- I will never post photographs or video clips without permission and never include names with the photographs.
- I will not copy text, images, sounds, animations, videos or music that breaks copyright laws.
- I will not sign up for any services or buy any goods.
- I will not access Internet chat rooms and instant messaging sites on school devices.

Email Use

- I will ask permission before opening an email or an email attachment sent by someone I do not know.
- I will only email people I know or my teacher has approved.
- **I will not be involved in sending chain letters.**
- The messages I send will be polite, friendly and sensible.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

Mobile Phone and hand held gaming devices

- I will not bring a mobile phone to school unless instructed by my parent and agreed by the school.
- I understand that my phone or hand held gaming device is my responsibility and that the school is not responsible if it is lost, stolen or damaged during the school day.
- I will switch my phone off and put it out of sight when entering the school grounds.
- I will not use my mobile phone during the school day. I will communicate through the school office if I need to make contact with my parents/carers during the school day.
- I will not bring hand held gaming devices to school unless permission has been granted by the teacher or principal.

Video Conferencing/ Face Time

- I will not initiate, make or answer video conferencing calls.
- I will follow agreed rules for video conferencing and class rules.
- I will maintain acceptable standards of manners, behaviour and language throughout.
- I will avoid causing disruption by e.g. staying in the room throughout the whole session and making sure I have visited the toilet before the lesson.
- I will listen to whoever is speaking/ take turns to speak/ respect what others say.

Consequences

I understand that if I deliberately break these rules, I may not be allowed to use email, the Internet or computers/ iPads.

There may be additional consequences in line with class rules on inappropriate language or behaviour.

Where applicable, police or local authorities may be involved.

Parents/ Carers

By signing this Acceptable Use Policy Document Parents/ Carers are agreeing to their child's use of the Internet in school based on the following statements.

- The school uses two Internet connections (C2K and iTeach) that have thorough security filters installed but cannot guarantee complete security and therefore still pose a small element of risk to pupils.
- The use of the Internet in school is closely monitored by staff and this will be in full view of others e.g. in a classroom or corridor.
- Parents/ Carers will cooperate with staff to make pupils aware of the rules and expectations within this document.
- The use of computers is complimentary to the teaching already done i.e. computers are a tool for learning in the classroom.
- No photographs of pupils will be available online without parents giving their permission.
- Children's full names will not be available online at any stage but some indication of work they do could be added to the school website to celebrate success. E.g. a poem that wins a prize in a competition may be posted on the class page of the website.
- Parents should discourage pupils from bringing mobile phones to school on the grounds that Internet access becomes very difficult to police. Where parents give pupils permission to bring their phones to school they will remind their child to adhere to the mobile phone rules outlined above.
- Parents should be aware that some social networking sites such as Instagram and Facebook adhere to a strict 'over 13's' age policy.
- Parents are advised to be present if their children are using gaming sites outside of school.
- Internet issues will be handled sensitively to inform parents without alarm.
- Further information can be found in the Parents E-safety section of the school website or by contacting the ICT Coordinator (Miss McCartney).

School

Use of the Internet in Grange Park Primary School safely is based on the following principles.

- All pupil internet access will be supervised by a member of staff.
- All Internet access will be via the C2K or iTeach filtered networks.
- Teachers will guide pupils towards appropriate materials and where possible check searches and websites prior to lessons.
- Tasks using the Internet will be carefully planned and linked to curriculum topics.
- Children will be taught how to use the Internet safely and responsibly through ICT and PDMU lessons.
- Pupils will be informed that Internet use is monitored and individual users can be traced and emails are filtered.
- Pupils in P1-3 will be shown how to log in using a simplified username and password. Pupils in P4-7 will use a unique C2K username and password to log in to the computers. In both instances the teacher will keep a note of the passwords.
- The ICT Coordinator and Principal are system administrators and therefore can access and restrict a pupil's account.
- All staff in school will make sure mobile phones are switched off and out of sight during teaching hours. Outside of directed time staff may use their phones when not in contact with children e.g. in the staffroom at lunch time.
- Teachers using video conferencing must revisit and agree protocols before a session occurs.
- In the computer room and classrooms there will be a display of computer rules and an e-safety incident flow chart.
- Staff will know and use the procedures for reporting e-safety issues.

A full copy of the school's E-safety Policy is available on request.

Grange Park Primary School

Three Way Agreement for Safe, Effective and Acceptable Use of Internet and Digital Technologies/ E-safety

Pupils Agreement

I have read and understand the school rules for digital technology use. I will use digital technology in a responsible way and will obey these rules at all times.

Signed by Pupil:

Class:

Date:

Parent's/ Carer's Consent for Internet Access

I have read, understood, and discussed with my child the school rules for responsible digital technologies use and give permission for my son/ daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities. I give permission for my son/ daughter to participate in carefully planned lessons that use Video Conferencing Technology under the supervision of their teacher. I will reinforce the safety precautions outlined in the pupil document above with my child/ren.

Signed by Parent:

Date:

Staff Guidance – What to do if…

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama, ask pupil to move away from computer/ switch screen off.
2. Note down details or website address/ content and intention of Internet use in lesson (i.e. what should the pupil have been searching for?)
3. Report to the Principal/ ICT Coordinator and decide whether to inform parents of any children who viewed the site.
4. ICT Coordinator will inform the c2kni helpline on 08706011666 and they will ensure the site is filtered.

An inappropriate website is accessed intentionally by a child.

1. Ask pupil to move away from computer/ switch screen off.
2. Note down details or website address/ content and intention of Internet use in lesson (i.e. what should the pupil have been searching for?)
3. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
4. Notify the Principal/ ICT Coordinator who may also notify Designated Child Protection Officer.
5. Notify the parents of the child.
6. ICT Coordinator will inform the c2kni helpline on 08706011666 and they will ensure the site is filtered.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the Principal and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the Principal should then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the school's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (contact Personnel/Human Resources).
   - Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local police or High Tech Crime Unit and follow their advice.
   - If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message and reassure them.
2. Listen to everything the child tells you of the incident and make a written report afterwards.
3. Secure and preserve any evidence.
4. Notify the Principal/ ICT Coordinator/ Child Protection Officer including all details of incident.
   Further Steps may include:
5. Inform the sender's e-mail service provider.
6. Notify parents of the children involved.
7. Consider delivering a parent workshop for the school community.
8. Inform the police if necessary.
9. Inform the relevant officer at SEELB

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

1. Secure and preserve any evidence.
2. Notify Principal/ ICT Coordinator with specific details of who is involved and evidence.

Further Steps may include:

3. Inform and request the comments be removed if the site is administered externally.
4. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
5. Endeavour to trace the origin and inform police as appropriate.
6. Inform SEELB

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the designated teacher for child protection or the Deputy in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform SEELB officer for Child Protection.
6. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Principal and teacher in charge of e-safety.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Staff Agreement of Safe, Effective and Acceptable Use of Internet and Digital Technologies/ E-safety

To be read and signed by all staff members of Grange Park Primary School.

I (staff member) have read Grange Park Primary School's E-Safety Policy and agree to the following statements based on the policy and will practice accordingly:

- E-safety is the responsibility of all stakeholders in Grange Park P.S. - any concerns should be reported immediately to the ICT Coordinator/ Child Protection Officer/ Principal.
- Not all risks can be eliminated by Internet filtering so I will therefore endeavour to follow recommendations in E-safety Policy. I am also aware that the use of the Internet must have clear expectations for enhancing the learning and be used in a structured way to minimise the risk for pupils.
- **Email –** School related correspondence should be through the monitored C2K email system or Gmail accounts. Emails should be of a professional tone and comply with the recommendations in E-Safety Policy.
- **Website –** The school website is to share the life of the school but also protect the **anonymity** of staff and pupils and therefore names and personal details should not be posted.
- **Mobile Phones/ Wearable Technology –** The use of mobile phones and wearable technology is prohibited during teaching time and should be out of sight of pupils during the rest of the school day. On school trips I may be asked to send a minimal number of photographs to the Principal for Twitter from my mobile phone. I understand that I am under no obligation to do this but if I do I should delete any images in the presence of a member of teaching staff as soon as possible after their use.
- **iPads –** I have read the Teacher iPad Policy and understand that this E-safety Policy extends to my school owned iPad at all times.
- **Outside of School –** There should be a clear boundary between my professional and private life online. If my online activity causes potential embarrassment for the school or detrimentally affects the school reputation of any of its stakeholders the Board of Governors are entitled to take disciplinary action.
- **Password Security –** I will endeavour to keep my C2K, SIMS and iPad passwords confidential at all times.

I agree to attend any E-safety training offered within directed time to ensure I am up to date on risks and procedures.

I am aware that the Principal and Board of Governors monitor online activity and can deactivate an account if misused.

Name _____**Signed** _____ **Date** _____

Grange Park Primary School Teacher iPad Policy – School Supplied

Should the school supply an iPad for your teaching use, you agree to the following:

- Use of the iPad should be considered the same as any other technology tool provided by the school.
- To abide by the schools Internet and E-safety Policy with regard to iPad usage.
- You will provide a list of all Apps installed in the device to the ICT Coordinator on demand. You will maintain this list with new downloads.
- To ensure that all apps meet with the requirements of the ICT and E-safety Policies.
- To inform the ICT Coordinator of any apps that do not meet said requirements and remove them from your device.
- To enforce a security passcode on the device and provide this on demand to the Principal.
- To ensure that the security passcode is confidential in line with E-Safety Policy.
- To use only the school Apple account for app downloads which have been approved by Principal or ICT Coordinator.
- To not use the device to store personal documents such as video or audio material other than that which is directly related to your school needs.
- To not install any apps which may be considered only for personal use, or could be deemed not suitable in the classroom.
- Use of the camera only permitted in line with the whole school Child Protection Policy and E-safety Policy.
- To report loss, theft or other damage occurring outside of school to the Principal as soon as possible and to make good the iPad to its original state. (In agreement with school.)
- That you will not sync or attach the iPad to your home or personal computer.
- You will not remove profiles or restrictions placed on the device.
- You will not 'jailbreak' the device.
- To purchase or use the provided case to protect the iPad for general day to day use.
- To not allow any pupil to use the iPad for any purpose except for curricular purpose under a controlled environment in the presence of a member of staff.

Further Information and Advice for Parents on E-safety

Grange Park Primary School would advise that all parents and carers consider Internet, Tablet and Computer use in their homes to ensure their children are safe online.

The following websites highlight some useful considerations.

- Advice about general Internet Use, Social Networking and online gaming and useful icebreakers for family discussions regarding Internet use.
  https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

- Keeping young children and young people safe online and an example family agreement for Internet use.
  http://www.childnet.com/blog/free-internet-safety-leaflets-for-parents-2016

- Advice on the issues of Internet use for children and information on Instagram security and advertising
  https://www.saferinternet.org.uk/advice-centre/parents-and-carers

- How to report online incidents that are causing concern and how to address this with your child.
  https://www.thinkuknow.co.uk/parents/

- Social media top tips
  https://www.internetmatters.org/advice/social-media/