Kesh Primary School
Achieving & Caring

KESH
NURSERY

Kesh Primary School
&
Kesh Community Nursery

E Safety Policy

Adopted by the Board of Governors……………………………

Signed ………………………………………………………………………………

Review……………………………………………………………………………….

(Amended after DENI circular 2016/27)

Table of Contents

1. Rational

2. Scope of Policy

3. Risk Assessment

4. Roles, Responsibilities and training

5. Current Practice

6. Technical Framework

7. Managing Incidents

8. Development, Monitoring and Review

9. Appendix

1. Rationale

“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 schools, 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 the Policy

This policy applies to all members of the 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 of 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. Any issues that arise inside school, as a result of E-Safety incidents outside of the School, will be dealt with in accordance with School Policies.

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, Contract 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 whom they may make contract 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.

4. Commercial

- The young child is exposed to inappropriate commercial advertising
- Exploitation due to marketing schemes and/or hidden costs/frauds

Many of these risks reflect situations in the offline world and it is essential that this E-Safety policy is used in conjunction with other School policies e.g. Positive Behaviour, Child Protection, Anti-Bullying and Acceptable Use, Mobile devices, Disposal of documents.
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 these risks.

4. Roles and Responsibilities

4.1 E-Safety Coordinator

The E-Safety Coordinators will lead the E-Safety Committee and takes day to day responsibility for E-Safety issues and have a leading role in establishing and reviewing the Schools policies/documents.

The E-Safety Coordinators will:

- 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 C2K, iTeach and school ICT technical staff
- Liaise with the ELB and DENI on E-Safety developments
- Liaise with the technical staff
- Receive reports of E-Safety incidents and create a log of incidents to inform future E-Safety developments
- Meet regularly with VP of pastoral care to investigate abuse of social network sites by pupils
- attend relevant meetings with Board of Governors
- discuss current issues, review incident logs
- monitors and reports to senior staff through the Vice Principal (Mrs. D Irvine; also and E-Safety Co-Coordinator) any risks to staff of which the E-Safety coordinator is aware
- oversees the application of the 360 Degree Safe Mark Award.

4.2 E-Safety Officers / Designated Child Protection Officer / Designated Deputy Child Protection Officer

The Child Protection Officer Mrs. D Irvine (who is also an e-safety coordinator) and Mrs. Gamble (Deputy Designated Child Protection Officer) will be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate online contact with adults / strangers
- Potential or actual incidents of grooming

- Cyber-bullying

4.3 E-Safety Committee

The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring of the E-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governors.

Committee Members:

- E-Safety Coordinators - Mrs. D Irvine and Mrs. Wendy Woods
- The Child Protection Officer - Mrs. D Irvine
- ICT Task Team – Mrs D Irvine, Mrs Wendy Woods and Mr Andrew Johnston
- ICT Coordinators– Mrs D Irvine and Mrs Wendy Woods
- Principal of School – Mrs. Jill Parkinson
- E-Safety Governor – Mrs Elaine Milligan
- Network Managers- – Mrs D Irvine and Mrs Wendy Woods
- iPad and iTeach liaison Managers – Mrs Gillian Cullen and Miss Kerrie-Jane Taylor

Members of the E-Safety Committee will assist the E-Safety Coordinators with:

- the production and review of the school E-Safety policy and related documents.
- mapping and reviewing the e-safety curricular provision, ensuring relevance, breadth and progression
- monitoring incident logs from the pastoral team
- consulting parents/carers and the pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 Degree Safe Self Review Tool

4.4 The Principal and Senior Leadership Team:

The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community though the day-to-day responsibility for e-safety will be delegated to the E-Safety Officers.

The Principal and E-Safety Officers/coordinators will be kept informed about e-safety incidents.

The Principal will deal with any serious e-safety allegation being made against a member of staff.

The Principal and SLT are responsible for ensuring that the E-Safety 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.

4.5 Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports.

NAME Mrs Elaine Milligan has taken on the role of the E-Safety Governor.

The designated E-Safety Governor is Mrs Elaine Milligan. She will:

- have regular meetings with the E-Safety Coordinators
- regularly monitor e-safety incidents logs

Training will be given to the Governors by:

- Attendance at training provided by relevant external agencies / staff in school
- Participation in school's training / information sessions for staff or parents

4.6 Network Managers - – Mrs D Irvine and Mrs Wendy Woods

The Network Managers will monitor that C2K e-safety measures, as recommended by DENI, are working efficiently within the school.

- that C2k/Classnet operates with robust filtering and security software
- that monitoring reports of the use of C2k / Classnet are available on request
- that the school infrastructure and individual workstations are protected by up to date virus software.
- that the school meets required e-safety technical requirements that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed the filtering policy is applied and that its implementation is not the sole responsibility of any single person that they keep up to date with E-Safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

- that the “administrator” passwords for the school ICT system, used by the Network Managers must also be available to the Principal and kept in a secure place

4.7 Teaching and Support Staff

The Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school E-Safety policy and practices.
- They have read, understood and signed the school’s Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the E-Safety Coordinator.
- Digital communications with students (email / Virtual Learning Environment (VLE) should be on a professional level only carried out using official school systems – either C2K or School Gmail accounts. Emails should be sent in accordance with the School’s guidance.
- E-Safety issues are embedded in all aspects of the curriculum and other school activities.
- Staff understand and follow the school E-Safety Policy and Acceptable Use Policy.
- That students have a good understanding of research skills and need to avoid plagiarism and uphold The Copyright, Designs and Patents Act 1998)
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, camera and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- Undertake all e-safety training as organised by the school

4.8 Professional Development for Teaching and Support Staff

Training will be offered as follows:

- All new staff will receive e-safety training as part of their Induction Programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- A programme of e-safety training will be made available to staff as an integral element of CPD. Training in e-safety will be supported within the PRSD or EPD process and where staff have identified a need.
- Staff will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
- This e-safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

4.9 Pupil E-Safety Committee

The pupil e-safety committee (sub-committee of the School Council) will assist the e-safety Officers with:

- Potential issues regarding e-safety
- Present information during an assembly on the Safer Internet Day and e-safety awareness week (which will occur annually in February)

- Pupils will only be expected to take part in staff committee meetings where deemed relevant.

4.9.1Pupils

Are responsible for ensuring that:

- They use the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to schools systems.
- They have a good understanding of research skills and the need to avoid plagiarism and uphold The Copyright, Designs and Patents Act.
- They understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They know and understand school policies on the use of mobile phone, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Pupils are introduced to email and taught about the safety and 'netiquette' of using e-mail both in school and at home.
- They 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 related to their membership of the school.

4.9.2 E-Safety Education for Pupils

E-Safety education for student will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT / PDMU / other lessons 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 as well as the school website link to www.thinkuknow.co.uk.
- Pupils will be taught in all relevant lessons 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
- Pupils will also be made aware of what to do if they feel unsure or unhappy about something that has appeared on their iPad/laptop/computer.

- Age appropriate e-safety tips are displayed in each classroom and also in resource Areas 2 and 3 where key Stage 1 and 2 utilise in allocated ICT times.

4.9.3 Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way and to support the E-Safety policy outlined by the School.

Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events. At every school event which images can be taken then the parent/carer **will be** asked to sign a form indicating that they have taken images for that particular event. These records will be kept in the school office for future reference. Also at each school event the Principal/Vice-Principal or adult in charge will remind all parents/carers to only put on social media photos of **their own child(ren).**
- online communication with staff
- their children's personal devices in the school (mobile phones/personal devices are not permitting in school unless for unavoidable circumstances – to which the parent must contact the school to discuss the circumstances, if permission is granted, then the child must understand to give the phone/personal device to the class teacher in the morning, who securely locks it away (school safe) and given back to the child at the end of the school day or when the child is leaving school.)

4.9.4 Parents / Carers Training and Support

Parents and carers have 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 will provide links to external sites such as CEOP, www.thinkuknow.co.uk and Digital Parenting
- Letters, newsletters, websites
- E-Safety Guidance will delivered through key events
- A designated E-Safety Parents' Evening
- Appendix 5: Internet Access: Additional Advice for Parents

4.9.5 Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUP before being provided with access to school systems.

4.9.6 Education for the Community

- The school will provide opportunities for members of the community to gain from the school's E-Safety knowledge and experience through:
- Providing family learning courses in use of new digital technologies, digital literacy and E-Safety
- The school website
- Supporting community groups e.g. library staff/sports/voluntary groups to enhance their E-Safety provision

5. Current Practice

5.1 Communication

- The official school email service may be regarded as safe and secure. Staff and pupils should therefore use the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Email communications with parents and/or pupils should be conducted through the following school email systems 'jparkinson663@c2kni.net'. Personal email addresses should not be used.

- 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.

- Any digital communication between staff and pupils or parents/carers - email, VLE and official school social media accounts - must be professional in tone and content. When emailing, staff should CC any communication to pupils to another member of staff.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

- Further information is provided to staff during in service training for appropriate use.

5.2 Social Networking

At present, the school endeavours to deny access to social networking sites to pupils during school hours.

- The school will provide training in the appropriate use of social networking / for teaching and learning purposes.
- Training will include: acceptable use; social media risks; checking of settings; data protection; reporting issues; legal risks.
- Teachers should adhere to the social networking / communication guidance provided by the school.
- Teachers will receive training in the appropriate use of social networking in their private life.
- Older students should be made aware of the appropriate and safe use of Social Networking.
- Teachers and pupils should report any incidents of cyber-bullying to the school.
- Further information is provided to staff during in service training, for appropriate use.

5.3 Pupils' use of personal devices

- In Kesh primary school we discourage children bringing mobile phones to school. Only in exceptional circumstances, after consultation with the principal will permission be granted. 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. Mobile phones will be kept locked in the school office and collected at the end of the day by the pupil. It is their responsibility to do so.
- Mobile Phones and personally-owned devices must be switched of. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If a pupil breaches the school policy then the phone or device 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 in accordance with the school policy.
- 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.

- Staff should **not** use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting parents, then a school mobile phone will be provided and used. In an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Further information is provided to staff/pupils/parents during in service training; also see the 'Mobile Devices Policy' Appendix 6: Use of Mobile Phones and other Electronic Devices for appropriate use.

5.4 CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission, except where disclosed to the Police as part of a criminal investigation.

We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5.5 Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with taking digital images and sharing on the Internet.

- When using digital images, staff informs and educates pupils about the risks associated with taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. Social Networking websites.
- The school gains parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school;

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- We will also ensure that when images are published that the young people cannot be identified by the use of their names.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- The use of digital / video images plays an important part in learning activities.
- The school will comply with the Data Protection Act by requesting parents' permission when their child starts school in Year, permission will last until the student leaves school, unless a parent / carer provides a written withdrawal of taking images of members of the school.

5.6 Teaching and Support Staff: Password Security

Password security is essential for staff, particularly as they are able to access and use student data.

- Staff are expected to have secure passwords which are **not** shared with anyone.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.
- Further information is provided to staff during INSET training.

5.7 Students: Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Acceptable Use Policy
- Students are expected to keep their passwords secret and not to share with others, particularly their friends.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Pupils are taught about appropriate use of passwords in each year group annually or at other intervals when deemed necessary; with particular focus from Year 3 to Year 7. In Foundation Stage the children log-on as a Foundation Stage User.

5.7 Cyber-bullying

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.

- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people. Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.
- Incidents of cyber–bullying will be dealt with in accordance with the School Anti-Bullying Policy.

5.8 The Data Protection Act

The school has a Data Protection Policy and staff are regularly reminded of their responsibilities. In particular, staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media, it is advisable that:

- the device is password protected
- the device offers approved virus and malware checking software
- the data is securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

5.9 Google Apps for Education

The school uses Google Apps for Education for pupils and staff. The following services are available to each pupil and hosted by Google as part of the school's online presence in Google Apps for Education:

- Mail - an individual email account for school use managed by the school for the children to log into Google Drive
- Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
- All pupils will have access to pre-approved downloaded Apps suitable to their Key Stage.

As part of the Google terms and conditions schools are required to seek parental permission for your child (under 13 years old) to have a Google Apps for Education account which will be sought at the beginning of Year 1. Any new pupils to the school will need parental permission. The permission may also be re-requested by the e-safety coordinators at any time deemed appropriate.

5.9.1 Technical Framework

Filtering of internet content provides an important means of preventing 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 Senior Leadership Team.

They manage the school filtering by:

- Monitoring reports of the use of C2k / Classnet which are available on request.
- Keep records and logs of changes and of breaches of the filtering systems.
- These changes and breaches should be reported to the E-Safety Coordinators.

Staff and pupils have a responsibility:

- to report immediately to any of the two E-Safety Coordinators 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.
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Auditing and reporting:

Logs of filtering change controls and of filtering incidents will be made available to:

- E-Safety Committee
- E-Safety Coordinators
- Board of Governors committee
- External Filtering provider / Police on request

7. Actions and Sanctions

Sanctions for the misuse of technology are outlined in the Acceptable Use Policy:

Appendix 6: Use of Mobile Phones and other Electronic Devices

Further to this, should technology or online platforms be used as a means by which to bully another, the sanctions detailed in the Positive Behaviour Policy will be implemented.

Level 2 sanctions:

- Inform parent through diary/phone call
- Meeting with parent(s) if necessary
- Loss of privileges – football, Golden Time
- Written apology or self-reflection using questioning – oral or written (no lines or extra work)
- Time out in classroom or other classroom (supervised)

Level 3 sanctions

- Principal informed immediately
- Risk assessment of situation
- Principal/SENCO/Designated Teacher Child Protection involved in monitoring
- Crisis/anger management and de-escalation interview
- Parent(s) contacted to meet Principal with class Teacher(DTCP/SENCO/e-safety coordinators)
- Note of concern regarding placement on SEN Code of Practice/Placement on SEN register foe EBD for Social Emotional and Behavioral reasons
- Other interventions – Targets, Daily Record Card etc., Nurture Group, Counselling
- Anger de-escalation strategies recognizing the stages of 'The Breakwell Cycle'

Level 4 sanctions

- Continued Placement on the SEN Register in line with Code of Practice (EBD)
- SEBD referral
- Other agencies e.g. CAMHs, EWO, Psychology
- Social and Emotional Behavioural Team involvement
- Suspension or exclusion following appropriate procedures (see suggested Roles and Responsibilities' – Ni Curriculum Guidance March 2014 – appendix 8 in Positive Behaviour and Anti-Bullying policy.

Further to this, should technology or online platforms be used as a means by which to bully another, the sanctions detailed in the Anti-Bullying Policy will be implemented.

'Intervention Strategies. The aim of any intervention applied is to RESPOND to the alleged incidents, RESOLVE the concern and RESTORE the well-being of all involved……

If proven, action will be taken to protect the 'child who has been bullied' and deal with the 'child who is displaying bullying behaviour' in line with the Positive Behaviour policy sanctions and involving all relevant staff on a need to know basis. Additional and complimentary levels of intervention are outlined in the (NIABF) file 'effective Responses to Bullying Behaviour' pages 16-19)

Parents/guardians involved will be given feedback using the school diary, by phone call or via parent – teacher meeting guided by pastoral team/principal. If the parent was the initial complainant a report back will be made (by phone call/interview) in line with the school complaints policy. Parents will be informed that they can contact the school again at any time if concerns are still evident.

The school is happy to direct parent, after consultation, towards appropriate counseling through external/internal agencies.

See also Appendix of the Ant-Bullying policy for examples of scripting, Bullying Incident Form, Northern Ireland Anti-Bullying Forum guidance Notes’.’

APPENDICES

Appendix 1: ICT Code of Safe Practice for Pupils

E Safety Rules

✓ I will log onto the My *School* Learning Platform with my own user name and password.

✓ I will only use ICT, including the internet, e-mail, iPad, digital video, mobile technologies etc. for school purposes.

✓ I will only use my class e-mail address or my own school e-mail address when e-mailing.

✓ I will only open e-mail attachments from people I know, or who my teacher has approved.

✓ I will not tell other people my ICT passwords.

✓ I will only open/delete my own files.

✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.

✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.

✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone through an online activity unless this is part of a school project approved by my teacher and a responsible adult comes with me.

✓ I will only take photographs on school devices when following teacher/adult instruction. I will not copy or send photographs without staff permission.

✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

✓ I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my e-Safety.

Pupil’s Full Name ……………………………………….... (printed) Class: ………………….

Pupil’s Signature …………………………….…………………. Date ……………………

Appendix 2: ICT Code of Safe Practice for Staff

ICT (including data) and the related technologies such as e-mail, internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs D Irvine (e-Safety Coordinator) or Mrs J Parkinson (Principal).

✓ I will only use the school's email or personal email (if approved by Mrs Irvine)/ Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.

✓ I will comply with the ICT system security and not disclose passwords provided to me by the school or other related authorities.

✓ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

✓ I will not give out personal details e.g. mobile phone number and personal e-mail address, to pupils.

✓ I will use the approved C2k secure e-mail system for school business.

✓ I will ensure personal data is kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Such data must be encrypted.

✓ I will not install any hardware or software on the C2K system without the permission of Mrs Woods/Mrs Irvine.

✓ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory on the C2K system or on the iPads.

✓ Images of pupils and/or staff will only be taken, stored and used for professional purposes online with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Principal.

✓ I understand that my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Mrs Woods or Mrs Irvine (managers).

✓ I will respect copyright and intellectual property rights.

✓ I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

✓ I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school.

Staff Member:………………………………………... Signature ……..……………….…. Date ……………………

Full Name ……………………………………... (printed) Job Title . . . .

Appendix 3: Parental Agreement/Consent Letter

Dear Parent/ Carer

It is essential that pupils are aware of e-Safety and know how to stay safe when using Information and Communications technology (ICT). As part of Kesh Primary School's ICT programme we offer pupils supervised access to a filtered Internet service provided by C2k (PCs and Laptops) and by iTeach (iPads). Access to the Internet enables pupils to explore and make appropriate use of many websites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However in spite of the tremendous learning potential, you should be advised that some material accessible, via the Internet, may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service providers C2k and iTeach have installed filtering software which operate by blocking thousands of inappropriate websites and barring inappropriate items, terms and searches in both Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

We would also like to remind you that any photographs/videos taken at school events by parents and placed on social media networks should only contain their own children.

The school's rules for safe Internet use accompany this letter. Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact Mrs Irvine.

………

Parent/ Carer signature

We have discussed this and …………………………………………(child's name) agrees to follow the e-Safety rules and to support the safe use of ICT at Kesh Primary School.

Parent/ Carer Signature …………………………………………………. Date ………………………

Appendix 4: Samples of Classroom Posters

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

□ We only use the internet when an adult is with us

□ We can click on the buttons or links when we know what they do.

□ We can search the Internet with an adult.

□ We always ask if we get lost on the Internet.

□ We can send and open emails together.

□ We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

e-Safety Rules for Key Stage 2

□ We ask permission before using the Internet.

□ We only use websites that an adult has chosen.

□ We tell an adult if we see anything we are uncomfortable with.

□ We immediately close any webpage we are not sure about.

□ We only e-mail people an adult has approved.

□ We send e-mails that are polite and friendly.

□ We never give out personal information or passwords.

□ We never arrange to meet anyone we don't know.

□ We do not open e-mails sent by anyone we don't know.

□ We do not use Internet chat rooms.

Principles for Internet Use (Children's Version)

Be SMART on Line

S	Secret: Never give out your address, telephone number, username or password when on-line.
M	Meeting someone or group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher.
A	Accepting e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent.
R	Remember no offensive language, text or pictures are to be displayed, sent, copied or received.
T	Tell your parent, teacher or trusted adult if someone or something makes you uncomfortable.

Smile and Stay Safe Poster

e-Safety guidelines to be displayed throughout the school

Smile and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to AGL (age, gender, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix 5: Internet Access: Additional Advice for Parents

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.
2. Parents should agree with their children suitable days/times for accessing the Internet.
3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use.
4. Parents should get to know the sites their children visit and talk to them about what they are learning.
5. Parents should consider using appropriate Internet filtering software for blocking access to unsavory materials. Further information is available from Parents' Information Network (address below).
6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities.
7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school they should immediately inform the school.

Further advice for parents is available from the following sources:

- http://www.thinkuknow.co.uk - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.

- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.

- http://www.parentscentre.gov.uk/using computers and the internet - A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.

- http://www.bbc.co.uk/webwise includes an 'Internet for Beginners' course and a tool for answering your internet related questions.

- http://www.kidsmart.org.uk/ explains the SMART rules for safe internet use and lots more besides.

- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)

- http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use

Appendix 6: Use of Mobile Phones and other Electronic Devices

Rationale
The Board of Governors of the Kesh Primary School wish to ensure that all pupils are safe and well cared for. All staff and pupils have a right to work, enjoy and learn in a secure and caring environment. They also have a responsibility to contribute to the protection and maintenance of such an environment. The use of increasingly sophisticated equipment and integrated cameras could present a number of problems, hence, the co-operation of parents and carers with this guidance is very much appreciated.

It is therefore school policy to prohibit the unauthorised use by pupils of mobile phones or other electronic devices while on our school premises, grounds or on trips or activities e.g. school swimming.

Guidance

The school will adhere to the following guidance:

- While we fully acknowledge a pupil's right to have a mobile phone or other electronic device, we discourage pupils from bringing them to school. They are valuable items and might be vulnerable to damage, loss or theft. There is also the potential for inappropriate behaviour and potential bullying which could be harmful to other pupils or staff. Many have built - in cameras which could lead to child protection and data protection issues with regard to inappropriate photographs or distribution of images. We have a duty to protect all members of our school community.

- In an emergency situation, and with the express approval of a senior member of the school staff, or where a written request has been received from the parent/carer, the device may be stored in the school office. It is the child's responsibility to ask for the device at the end of the school day. Should parents need to contact pupils, or vice versa, this should be done following the usual school procedures: via the school office (028 686 31441).

- Pupils may only take photographs on school devices as part of a supervised educational activity which has been authorised by a senior member of staff.

- The school accepts no liability for the loss or damage of any electronic device which is in the pupil's possession during the school day.

- If a pupil is found by a member of staff to be using a mobile phone/electronic equipment for any purpose, the device will be confiscated from the pupil. The pupil must arrange for their parents/guardians to collect confiscated equipment from the School Office during normal working hours.

- Inappropriate photographs or video footage with a mobile phone or other electronic device of other pupils or teachers will be regarded as a serious offence and disciplinary action will be taken.

- This policy supports the school’s Health and Safety and Safe Guarding Policies: Anti-bullying, Child Protection, Positive Behaviour and Internet Acceptable Use policies. It has been endorsed by the Board of Governors and will be monitored, reviewed and amended as required.

THINK U KNOW .CO.UK

Top Tips!

□ **Always ask a grown up** before you use the internet. They can help you find the best thing to do.

□ **Don't tell strangers** where you live, your phone number or where you go to school. Only your friends and family need to know that.

□ **Don't send pictures** to people you don't know. You don't want strangers looking at photos of you, your friends or your family.

□ **Tell a grown up** if you feel scared or unhappy about anything.

□ You can also call 'Childline' **on: 08001111** to talk to someone who can help.

Top Tips Taken from www.thinkuknow.co.uk