e-safety policy summary

2.0 WHAT IS e-SAFETY at Moyle PS and NU

e-Safety is short for electronic safety.

This policy highlights the responsibility of the school, staff, governors and parents/carers to mitigate risk through reasonable planning and actions. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology as well as collaboration tools and personal publishing.

e-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world;

- emphasises learning to understand and use new technologies in a positive way;

- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;

- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and

- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately.

6.0 HANDLING OF e-SAFETY

To deal with any incidents of technology misuse by pupils which arise, the school's Positive Behaviour Policy will be followed. Pupils must be made aware the repeated misuse of the Internet may lead to their access being denied. If a member of staff is involved, then the disciplinary procedures for employees of the school will be followed.

Where the incident involves child abuse, the Designated Teacher for Child Protection/Safeguarding Children in the school must be notified and the school will follow procedures as set out in the school's Child Protection/Safeguarding Children Policy.

Issues of Internet misuse and access to any inappropriate material by any user should be reported immediately to the school's e-Safety Co-ordinator and recorded in the school's e-Safety log, giving details of the site and the time.

A record of very serious e-Safety incidents will be kept in the locked Child Protection/Safeguarding Children cabinet within school.

Harassment of another person using technology, or breaching their right to privacy (e.g. reading their mail, accessing their files, using their computer account or electronic mail address), poses a threat to their physical and emotional safety, and may have legal consequences.

For these purposes, it is also essential that evidence of misuse is secured. If the school identifies a suspect device (containing for instance indecent images or offences concerning child protection), it will not be used or viewed and advice will be sought from the P.S.N.I.

After a minor or major incident a comprehensive debriefing will occur to review school policy and procedures.

Logs of misuse, changes to filtering controls and of filtering incidents are made available to the:

- Senior Leadership Team;
- Principal;
- Governors or governors' sub-committee;
- e-Safety Team.

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

8.0 ILLEGAL or INAPPROPRIATE ACTIVITIES

The school believes that the activities listed in the full policy and which will be obvious such as use of non-acceptable content etc are inappropriate (and on occasions illegal) in a school context and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

9.0 e-SAFETY AND PUPILS

Pupils need to know how to cope if they come across inappropriate material or situations online. e-Safety will be discussed with pupils on an ongoing and regular basis. This should be discussed with the pupils in an age appropriate way as a set of rules that will keep everyone safe when using technology in school. Refer to Appendix 2. It will also be discussed as they accept the agreement through their MySchool log in.

Activities to promote e-Safety awareness are taught throughout the school year and include participation in Safer Internet Day and visits from the PSNI reinforce e-Safety and further pupils' understanding.

Staff should always ensure that any Internet searches involving sites that have been granted enhanced access to should not be carried out when children can view them, i.e. on the computer's screen or on an interactive whiteboard. 'YouTube' should only be used after the content has been viewed and checked, ensuring that children are not exposed to inappropriate content.

11.0 e-SAFETY AND PARENTS/CARERS

The e-Safety policy will be published on the school's website and parents/carers will be encouraged to read the document. Moyle Primary School will look to promote e-Safety awareness within the school community which may take the form of information evenings for parents/carers, information leaflets and/or links on the school website.

Information is available on the 'Think U Know website': www.thinkuknow.co.uk

13.0 INTERNET USE

- The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.

- Educating pupils on the dangers of technologies that may be encountered outside of school will be discussed with pupils in an age appropriate way on a regular basis by teachers and other agencies (as appropriate – E.g. PSNI as part of the CASE project).

- Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of how to seek advice or help if they experience problems when online. E.g. from a parent/carer, teacher/trusted member of staff.

- The school internet access is filtered through the C2K managed service.

- Use of the internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.

- Pupils will be taught to use the internet as an aid to learning.

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

- Children will be taught to be 'Internet Wise' and therefore good online citizens and are encouraged to discuss how to cope if they come across inappropriate content.

14.0 E-MAIL USE

- The C2k Education Network filtering solution provides security and protection to C2k email accounts. The filtering solution offers scanning of all school email ensuring that both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

- Pupils must immediately tell a teacher when using their C2K email address (if activated) if they receive an offensive e-mail.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- Children will not always be given individual C2K e-mail addresses. In some instances, children may have access to a group e-mail to communicate with other children as part of a particular project. Messages sent and received in this way will be supervised by the teacher.

15.0 SCHOOL WEBSITE/FACEBOOK PAGE

Moyle Primary School's website and 'Facebook' page promote and provide up-to-date information about the school and showcase other aspects of school life. In order to minimise risks of any images of pupils on the school website and 'Facebook' page being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions;

- Only photographs of children with parent/carer consent will appear on the school's website.

- Names will be included with photographs on the website only if parent/carer permission has been given;

- The website / 'Facebook' page does not include home addresses, telephone numbers, personal e-mail or any other personal information about pupils or staff.

- The point of contact to the school i.e. school telephone number, school address and email address.

16.0 SOCIAL NETWORKING

Social software is a generic term for community networks, chat rooms, instant messenger systems, online journals, social networks and blogs (personal web journals).

Social environments enable any community to share resources and ideas amongst users. There are many excellent public examples of social software being used to support formal and informal educational practice amongst young people and amongst educators. They are also popular ways of enabling users to publish and share information, including photographs, video from webcams, video files and blogs about themselves and their interests.

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

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

- The school C2K system denies access to social networking sites.

- Pupils and their parents/carers are advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.

- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

- Cyber-bullying is addressed within this policy and staff are made aware that pupils may be subject to cyber-bullying via electronic methods of communication both in and out of school. (More information provided below).

- Our pupils are asked to report any incidents of cyber-bullying to the school.

19.0 MOBILE PHONES AND OTHER RELATED TECHNOLOGIES

It is important to be aware of the safety issues regarding mobile phones and other devices which now increasingly have Internet access. For this reason, Moyle Primary School has a specific policy on the acceptable use of mobile phones and related technologies.

If mobile phones or other related technologies are brought into school by pupils, it is our policy that they should remain switched off during the time the pupils are on the school's premises. If a mobile phone is switched on and used inappropriately, for example, cyber bullying, sending inappropriate text or images, the school's 'Positive Behaviour Policy' and if appropriate, 'Child Protection/Safeguarding Children Policy' 'will be adhered to.

Staff members should refrain from using their mobile phones or similar technology when in contact with children unless prior permission has been given by the Principal.

If photographs of pupils are being used by staff for lessons, presentations, website design etc., then they should be stored as much as possible on the C2K system. If however, staff are working on school related activities on personal computers, any photographs stored should be kept to a minimum and transferred to the school's network system as soon as possible. Photographs stored on a teacher's personal computer for school purposes should be deleted as soon as possible after they are no longer required or transferred to the school's C2K system.

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

Cyber Bullying

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

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content;

- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity;

- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile;

- Online Gaming – abuse or harassment of someone using online multi-player gaming sites;

- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people;

- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

It is important that pupils are encouraged to report incidents of cyber-bullying to both the school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases. Pupils are also encouraged to click the 'Report Abuse' link which is available on social media

A record is kept of all incidents of cyber-bullying in the school's e-Safety log. This allows the schools e-Safety team to monitor the effectiveness of the school's preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

ACCEPTABLE USE OF THE INTERNET: GUIDELINES for PUPILS

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

Staff should continually teach and stress the importance of safe use of the internet. WHEN USING THE C2K SYSTEM PUPILS SHOULD:

- only use their own login username and password;

- use the Internet for school/educational purposes only;

- tell a teacher immediately if he/she sees anything that they consider inappropriate or receive messages they do not like;

- only send e-mail or any other form of electronic communication in school when directed by the teacher;

- make sure any internet based communication is polite and responsible;

- understand that if they consistently choose not to comply with these expectations

they will be warned and subsequently may be denied access to Internet resources;

- understand that the school may check their computer files/e-mails and may monitor the Internet sites that they visit when on school systems.

WHEN USING THE C2K SYSTEM PUPILS SHOULD NEVER:

- access other people's files without their permission;

- change or delete other people's work/files without their permission;

- provide personal information such as telephone numbers and addresses when using the Internet;

- use electronic communication to arrange to meet anyone;

- use Social Media or equivalent while in school;

- bring in memory devices from home to use in school unless given permission by a member of staff;

- use any personal electronic devices they have their possession within school to access the internet or any messaging services unless permission has been given by a member of staff.