Online Safety Policy

Revised June 2016

Note: April 2017

This policy is under review as part of Shared Education (Teacher Professional Learning) Project with Castledawson PS

Expected date of completion: November 2017

Online Safety Policy

New Row's Online Safety Policy reflects the importance we place on the safe use of information systems and electronic communications. Online Safety (Electronic Safety) highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. Online Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using Information Technology.

E-safety:

- 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 educating children about the risks as well as the benefits so that users feel confident online.
- Is concerned with supporting children and young people 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.

The rapidly changing nature of the Internet and new technologies means that Online Safety is an ever growing and changing area of interest and concern. Our school policy must reflect this by keeping abreast of the changes taking place. We as teachers have a duty of care to enable pupils to use on-line systems safely.

Professional Development for Teachers:

Teachers are the first line of defence in e-Safety. Our observation of behaviour is essential in recognising concerns about pupils and in developing trust so that issues are reported. Staff will avail of training and support to determine what action is appropriate including when to report an incident of concern to the school Designated Teacher for Child Protection. Online Safety training is therefore an essential element of staff induction and should be part of an on-going continuous professional development programme. Guidance may be obtained from organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

Education of Pupils:

The Internet is an integral part of pupils' lives, both inside and outside school. There are ways for pupils to experience the benefits of communicating online with their peers, in relative safety. All key stage 2 pupils will partake in the BECTA Internet Proficiency Scheme. Primary 6 & 7 pupils will also receive a talk from the PSNI about how to stay safe online. Children should be taught to think SMART thus knowing that:

- they should never give out personal details,
- they should never arrange to meet anyone contacted via the Internet,
- they should not accept requests or mail from people they do not know,
- people are not always who they say they are,
- they should tell someone if someone or something makes them feel uncomfortable when online.

These S.M.A.R.T. targets will also be displayed on notice board inside the computer suite.

Risk Assessments:

New Row will perform risk assessments on the technologies within our school to ensure that we are fully aware of and can mitigate against the potential risks involved with their use. Pupils must know how to cope if they come across inappropriate material or situations online. Our school risk assessments should inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.

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. This form of bullying should be considered within schools overall anti-bullying policy, pastoral care policy and cyber bullying policy.

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. It is important that pupils are encouraged to report incidents of cyber-bullying to both school and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

We will also keep a record of cyber-bullying incidents to monitor the effectiveness of our preventative activities and to review and ensure consistency in our investigations, support and sanctions.

Communication of our Online Safety Policy:

This policy, supported by the school's Acceptable Use Agreement for staff, visitors and pupils, is to protect the interests and safety of the whole school community. All teachers and parents have received a copy of the Online Safety Policy and thereafter parents of primary 1 will receive a copy included in their welcome pack. A copy of the Policy will also be available on the school's website. This policy and its implementation will be updated on a regular basis.

Online Safety rules are displayed in all classrooms and in the ICT suite. They will be discussed with the pupils at the start of every year.

Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons / circle time/ anti-bullying week/ Safe Internet Day.

Parents/carers are asked to read through and sign the acceptable Use Agreement on behalf of their child. It is hoped that the school website will contain useful information and links to sites like CEOP'S thinkuknow, Childline and the CBBC Web Stay Safe page.

E-mail security:

We strongly advise against the use of personal e-mail accounts. Instead we encourage all users to use their C2K email as the C2K Education Network filtering solution provides security and protections to all C2K e-mail accounts. The filtering solution offers scanning of all school e-mail ensuring both incoming and outgoing messages are checked for viruses, malware, spam and inappropriate content.

Internet Security:

Staff and pupils accessing the Internet via the C2K Education Network will be required to authenticate using their C2K username and password. This authentication will provide Internet filtering via the C2K Education Net work solution.

Access to the Internet will be supervised at all times. Access via the C2K Education Network is also fully auditable and reports are available to the school principal.

Publishing Pupils' Images and Work:

Written permission from parents or carers will be obtained before photographs of pupils are taken and published. This consent form is considered valid for each academic year unless there is a change in circumstances. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.