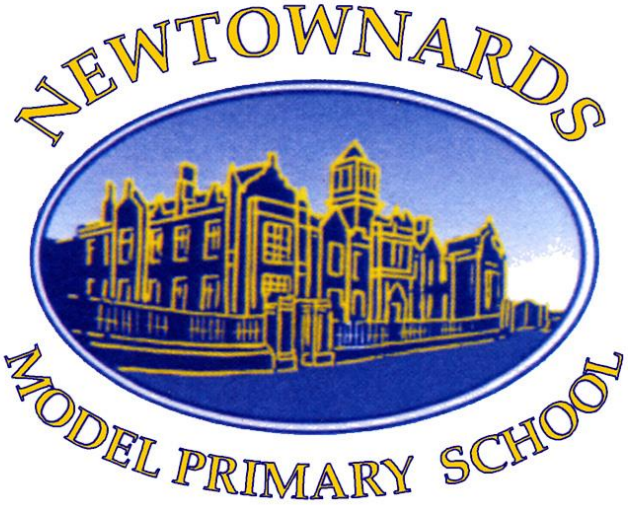
SCHOOL POLICY
FOR
Information and Communications Technology



NEWTOWNARDS MODEL PRIMARY SCHOOL

Newtownards Model Primary School ICT Vision

- To provide opportunities to enable all our staff, pupils and parents to be confident, competent and independent users of ICT.
- To provide an environment where access to ICT resources is natural and commonplace.
- To ensure ICT has a fundamental role in developing and enhancing our school's key learning aims in promoting the pupils' educational, physical and social needs.
- ICT encourages our staff and pupils to work collaboratively.

1. Purpose

This policy reflects the school values and philosophy in relation to the teaching and learning of ICT. It sets out a framework within which teaching and non-teaching staff can operate and gives guidance on planning, teaching and assessment.

The policy should be read in conjunction with the scheme of work for ICT which sets out in detail what pupils in different classes and year groups will be taught and how ICT can facilitate or enhance work in other curriculum areas.
This document is intended for:

- All teaching staff
- All staff with classroom responsibilities
- School governors
- Parents
- Inspection teams

2. Rationale

Information and Communications Technology (ICT) is changing the lives of everyone. ICT is a generic term used to denote the convergence of computers, video and telecommunications, as seen in the use of multi-media computers, mobile phones, gaming consoles etc.

We recognise that ICT is an important tool in both the society we live in and in the process of teaching and learning. Pupils learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources.

- ICT provides opportunities to enhance and enrich children's learning experiences across the curriculum
- ICT can present information in new ways, which help pupils to understand, assimilate and use it more readily
- ICT gives pupils access to immediate and up-to-date sources of information
- ICT can motivate and enthuse pupils
- ICT has the flexibility to allow pupils to work at their own pace
- ICT offers potential for effective individual/group/whole class work
- ICT gives pupils opportunities to develop skills for life
- ICT encourages learners in research based, flexible and effective forms of learning that will contribute to lifelong learning

3. Aims of ICT

We aim:

- To raise levels of pupil competence and confidence in using ICT - by developing children's knowledge, understanding and skills in using a range of ICT tools to enhance learning experiences across the curriculum
- To use ICT to enhance and enrich children's learning and add to its enjoyment
- To develop a whole school approach to ICT ensuring continuity and progression in all strands of the Northern Ireland Curriculum.
- To raise levels of teacher competence and confidence in integrating ICT into their planning, teaching and assessment of children's work (using ICT as an integral part of the processes and the management of teaching and learning)
- To provide access to electronic sources of information and interactive learning resources
- To enable children and teachers to have access to immediate and up-to-date sources of information
- To develop children's independent learning skills using ICT across the curriculum
- To develop information handling and research skills
- To ensure ICT is used, when appropriate, to improve access to learning for pupils with a diverse range of individual needs, including those with SEN and disabilities.
- To maximise the use of ICT in developing and maintaining links between other schools, the local community including parents and other agencies.

4. Resource Provision and Organisation

Newtownards Model Primary School is well equipped with ICT resources which are deployed throughout the school to maximise access, to enhance teaching & learning and to raise attainment. To enable regular and whole class teaching of ICT the school has an ICT suite comprising 31 networked PCs which all classes use weekly. All PCs provide internet access as well as over 70 software titles to suit curriculum needs.

To support the cross curricular nature of ICT every class also has access to

- a minimum of two class PCs with internet connection
- a colour printer
- a digital camera
- an iPad
- an Interactive Whiteboard

Ceiling mounted projectors are also located in the Computer suite, Art suite and the assembly hall along with Interactive Whiteboards in the dining hall and learning support rooms. These are used as a teaching resource across the curriculum. Each teacher has both a laptop and iPad for use in class and there are laptops and iPads available within the school for pupil access.

Other ICT equipment includes webcams, USB microphones, DVD players, calculators, digital video cameras, programmable toys such as Bee-Bots and Pro-Bots, scanners and electronic microscopes. As children progress from P1-P7 they are given opportunities to use a variety of these ICT resources. All equipment, serial numbers and locations are listed on the 'Equipment Log.'

5. Access

Pupil Access

- Through C2K computers all pupils have access to software titles appropriate to their curriculum needs and learning needs
- All children have access to the Internet
- Through the network, children in each classroom have access to printing facilities
- Where appropriate, pupils with Special Educational Needs will have access to specialist equipment or software to enable them to access the ICT resources fully.

Children use ICT resources under the guidance of the teacher and the use of the Internet is always a supervised activity. Although the school offers a safe online environment through filtered internet access we recognise the importance of teaching our children about online safety and their responsibilities when using communication technology. For all information related to this see our e-Safety policy.

Teacher Access

- All teachers have access to the C2K system
- Through My-School all teachers have access to their files, school email and software appropriate to their curriculum planning needs and classroom practice from any device
- Through C2K computers/laptops and mobile devices all teachers have access to the Internet
- All teachers have access to laptops available for use on the network and for home use
- All teachers have access to ICT equipment such as USB microphones, interactive whiteboards and digital cameras to facilitate a variety of teaching approaches

6. Strategies for Using ICT Resources

- ICT is taught as a distinct subject, but it is also a tool to be used as appropriate throughout the curriculum
- All pupils are given equal access
- ICT is an entitlement for all pupils
- Common tasks are set that are open-ended and can have a variety of responses
- We provide suitable learning opportunities for all children by matching the challenge of the task to the ability and experience of the child
- Use of ICT at home will continue to be encouraged through projects, homeworks and the use of My-School and Fronter which can be accessed though a home computer, tablet, smart phone or at the local library
- Children should continue to be encouraged to access and make use of the school website which is regularly updated – www.newtownardsmodelprimary.co.uk/

Where appropriate, children will have opportunities to use ICT resources to carry out:

- Individual work
- Group activities
- Whole class activities - Children may share in a computer-led activity using the interactive whiteboard and during lessons in the computer suite

7. Planning

Planning at Whole-School Level

- The Principal, SMT, ICT Co-ordinator and staff consult on how ICT is incorporated into the School Development Plan
- In consultation with all staff an ICT Action Plan is drawn up annually by the ICT Co-ordinator and is reviewed by all staff as appropriate
- A line of development in ICT ensuring progression and continuity for children in each of the '5 es' from P1-P7 has been drawn up and agreed by all staff

Planning at Year-Group and Class Level

Our six-weekly plans for ICT will be used by each teacher and they will make adaptations to ensure the plan is progressive in developing pupil capability in each of the '5 es'. These are used as working documents which are evaluated each half term to identify additional resource needs and to review the success of activities undertaken. These plans are integrated to ensure that delivery of ICT is linked to topics and other curriculum subjects. Plans will include a variety of teacher-prepared activities as well as CCEA Using ICT tasks.

Teachers meet in year groups to discuss and review progress, share experiences of using ICT, look at samples of children's work and discuss effectiveness of planning.

The 'Five Es'

Newtownards Model Primary School meets the requirements set out within the Northern Ireland Curriculum and develops the use of the 5Es within the tasks already being carried out:

Across the curriculum, at a level appropriate to their ability, pupils will be enabled to:

Explore

- access, select, interpret and research information from safe and reliable sources;
- investigate, make predictions and solve problems through interaction with digital tools.

Express

- create, develop, present and publish ideas and information using a range of digital media and manipulate a range of assets to produce multimedia products.

Exchange

- communicate safely and responsibly using a range of contemporary digital methods and tools, exchanging, sharing, collaborating and developing ideas digitally.

Evaluate

- talk about, review and make improvements to work, reflecting on the process and outcome, and consider the sources and resources used, including safety, reliability and acceptability.

Exhibit

- manage and present their stored work and showcase their learning across the curriculum, using ICT safely and responsibly.

8. E-Learning

E-learning is learning that is made possible and supported through the use of Information and Communications Technology (ICT) in school and at home. Undoubtedly, eLearning involves engaging in a wide range of learning activities, both inside and outside school, including the use of ICT to support life-long-learning for families.

Virtual Learning Environments

We will be developing our Virtual Learning Environment (VLE) in Newtownards Model Primary School. We are using the computer-based learning environment called Fronter run by C2K. The advantage of online learning means that it can be accessed from any computer with internet access in the world.

Fronter is a learning platform which supports learning & teaching, collaboration & communication. It offers a wide range of functionality including 5 types of discussion forum as well as hand-in and portfolio tools so teachers can monitor students' activity and progress. Teachers can support students with organisation by adding reminder messages to the home page.

Fronter integrates with Equella the new C2k Digital Content Repository. The platform offers an attractive interface and teachers can use a webpage-style navigation approach to provide an engaging path through learning activities.

9. Assessment, Recording and Reporting

Children's use of ICT is assessed and recorded by the classroom teacher using the following approaches:

- Formative assessment methods - observing and questioning during classroom activities
- Summative assessment methods - in collecting samples of children's work using ICT
- Self-Assessment – the children will assess their own skills each year using a self-assessment sheet appropriate to their level and set themselves targets accordingly
- At the end of KS1 and KS2 the children's work will be formally assessed using CCEA tasks and other class activities to assign levels. We aim to build on this process by developing and maintaining electronic portfolios of pupils work and holding moderation meetings to ensure accurate levelling.

Teachers will report on a child's progress:

To the Next Teacher:

- By discussing progress
- By passing on samples of work
- By passing on information regarding skills/level

To Parents/Carers:

- By informal discussion during parent interviews
- By a formal comment regarding ICT Competence on the child's written report

10. Provision for Pupils with Special Educational Needs

It is important to recognize the potential of ICT to help address children's individual learning needs. ICT is used to enhance the learning experiences of children with special educational needs within the school.

- Where appropriate specialist hardware equipment, such as a touch screen, big mouse, big keyboard etc. will be made available to meet a child's needs
- Where appropriate, specific software e.g. Wellington Square, Talking Word Processors, are used to assist learning
- Where appropriate, teacher developed resources such as Clicker 5 word banks are used to assist learning

Teachers will familiarize themselves with the variety of graded levels within frequently used software in order to provide differentiation and cater for children with special educational needs within their classrooms.

The Learning Support team have access to networked laptops to support their everyday teaching and learning strategies.

The use of ICT to provide challenge for Gifted and Talented children is also explored.

11. Equity of Access

All children will have equity of access to the use of ICT across the curriculum. The school will guard against gender stereotyping with encouragement given to both girls and boys to engage in ICT related activities. Children of all ages, ability levels, and backgrounds will have equal access to ICT resources.

It is important that children who do not have ICT resources at home should not be disadvantaged. A computer and a digital animation club operate after school on a weekly basis. We believe this access to ICT out of school hours:

- increases the time our children spend learning;
- increases access to ICT especially for those children without a computer at home;
- enables some children to develop and extend personal hobbies and interests;
- develops ICT capability; potentially raising self esteem, motivation and standards of achievement.

12. ICT in the Home and in the Community

Children are given the option to complete some homework tasks, when appropriate, using ICT out of school. Teachers are sensitive to the fact that children may not have access to ICT or may not wish to use it to complete tasks out of school.

A school email address has been given to parents and is listed on the school website. More parents are now using this to contact staff, arrange meetings etc. Our school website promotes the school's achievements as well as providing information and communication between the school, parents and the local community.

In keeping with the school Homework Policy children will be encouraged to make use of home computers and ICT resources available through places such as After School Clubs, Libraries, and Youth Clubs.

Where appropriate children will be given opportunities to make use of ICT resources to:

- Carry out research to support classroom work, projects etc.
- To complete work begun in school
- To carry out or present a homework task

Work carried out on home computers should be valued. It is important to ensure that a consistent approach to children's use of home computers is taken in each class as a child progresses through the school.

As indicated in our approach to equity of access, children who do not have ICT resources at home should not be disadvantaged.

13. Health & Safety

Employers have the legal responsibility for health and safety in schools, but in practice teachers do much of the day-to-day work to ensure that ICT equipment is used correctly and safely. It is important, therefore, that teachers are aware of the health and safety issues associated with information and communications technology (ICT). The Health and Safety (Display Screen Equipment) Regulations 1992 apply to users who use display equipment as a significant part of their work. This may apply to staff working in the school office.
Pupils should only be allowed to connect or unplug electrical equipment after proper instruction, and always under the supervision of the teacher. A major cause of accidents in computer suites is baggage left lying around which can cause pupils to trip. Ensure that storage is adequate and within safe reach.

Safety Issues to be Considered:

Comfort
Users should be comfortably positioned with easy access to all equipment. Whilst sitting, it is essential that the user can adjust his or her position in relation to the equipment as appropriate. Users should take frequent short breaks from computer work, such as a 10-minute break every hour, to allow eyes to readjust to greater distance.

Space

There should be enough space around a workstation for peripherals such as papers, books or other materials, including special education needs equipment such as concept keyboards. There should also be space for more than one pupil at a time and for the teacher to gain access. It is important to ensure that gangways and emergency exits are kept clear. Try to position workstations away from doorways where traffic is heavy, away from corners where lack of space might be awkward, and away from radiators where the heat might make it uncomfortable for pupils.

Seating

The height of the chair should be adjustable, bearing in mind that users should be aiming for good posture when operating computer equipment. Ideally, the height and tilt of the back of the chair should also be adjustable. The lower arms should be roughly horizontal when working, and knees should fit comfortably under the desk, with thighs roughly horizontal. Footrests should be available as necessary to reposition legs. Change posture frequently and take short breaks away from the
computer to stretch.

Monitors

These should tilt and swivel to suit the requirements of individual users. Screens should be positioned to reduce reflections and glare from lights and windows. The top of the screen should be roughly at eye level. Users should also be able to control brightness and, for many, comfort is increased if they can adjust screen colours and type fonts. There may be screen distortion if speakers are situated too close to the monitor. It is advisable, therefore, to position speakers about one foot away from the
computer.

Electrical safety

Under the Electricity at Work Regulations 1989, all electrical equipment should be maintained regularly. Always leave technical repairs to the experts. Ensure that you have the necessary CO2 fire extinguishers positioned near any ICT equipment.

The location of electrical equipment depends on the length of cables and the availability of sockets for telephones, TV aerials and power. It is essential that the location of the equipment does not increase the risk of danger to equipment or users.

Particular issues to be aware of are as follows:

• Cover and secure trailing power cables.

• Replace frayed leads or damaged plugs.

• Do not overload circuits, particularly when using long extension leads, as power surging can occur if too many computers are connected to a circuit, or when electrical floor cleaning equipment is plugged in.

• Avoid coiled cables, as the heat generated within them could be sufficient to start a fire.

• Be aware of accidental damage, in particular any cuts to power cable insulation, and also damage from dust, spilt liquid.

Ensure that the correct fuse rating is fitted. Ensure that keyboard and mouse connecting cables do not hang over the front of the computer workstation. Where the workstations are accessible from the rear, as in the case of trolleys, ensure that trailing loops of cable are tidied to allow easy access to equipment for maintenance and to prevent equipment from being dragged accidentally from the workstation by students.

The school should ensure that there is a system in place for regular visual checks of plugs, leads and other electrical equipment.

Mobile equipment

ICT equipment is often heavy or bulky, and the Manual Handling Operations Regulations cover this area. You will need to assess the risk of lifting heavy or awkward equipment and use trolleys where appropriate. It is better to push a trolley than to pull it.

When using mobile equipment such as televisions, projectors and screens around the school, ensure that the equipment is anchored firmly when in use, and that trailing power cables are covered and secured.

Hazardous substances

The Control of Substances Hazardous to Health Regulations cover this area, and risk assessment is necessary when using toners, printing inks and cleaning materials.

Toner that is used in printers and photocopiers is a fine dust. At one time, some toner was carcinogenic and may still be in use in some institutions. Careful handling required the use of gloves and special waste disposal. Inhalation should be avoided, as should contact with skin. It is important to check the manufacturer's instructions.

Fluids used for cleaning and in some reprographic processes are flammable. Always handle these with care and store in minimum quantities, preferably in metal containers, away from heat. Other substances, such as solvents, are dangerous to inhale. Care should always be taken to re-seal lids securely and store in upright containers. They should not be used in confined spaces, and adequate ventilation should be maintained.

Projector Health and Safety Issues

It is important that all users are aware of the health and safety implications of using projection equipment in the classroom, particularly if children might stand in front of the beam to give presentations. All projectors have the potential to cause eye injury; so some simple guidelines should be followed:

- No one should stare directly into the beam of the projector.
- When entering the beam, users should not look towards the audience for more than a few seconds.
- Users should keep their backs to the projector beam when standing in it.
- The use of a stick or laser pointer is recommended to avoid the need for the user to enter the beam.
- Children should be supervised at all times when a projector is being used and in particular when they are asked to point out something on the screen.
- Control light in the room by using blinds which diffuse rather than remove ambient lighting thus reducing the need to increase the beam intensity.
- Retaining some ambient light enables eye to eye contact to be maintained and there is some evidence that pupils work more ably when exposed to natural light. Restore natural daylight promptly on conclusion of interactive whiteboard sessions.
- Use the brightness reduction facility on the projection when a presenter is standing in front of the projector.
- A maximum of 1500 ANSI lumens should be more than adequate for most classroom environments.

- Projectors should be installed as far forward as possible to avoid the projector beam entering the user's field of vision. This is best achieved by ceiling-mounting, rather than floor— or table-mounting, the projector. There are also some all in one interactive whiteboards emerging which remove any potential danger of getting the light beam in the eye of the user and almost eliminates the area of shadow from the user.
- Board positioning should be determined following an appropriate risk assessment.
- Electrical standards and regulations apply in relation to all interactive whiteboards aspects.
- It is recommended that guidelines are displayed, as a reminder, adjacent to interactive boards.

Electrical Installations

All electrical installations undertaken, including whiteboards, should follow all local authority guidelines. In most cases these should follow the BS7671 and NICEIC standards. It is important to note that projector power installations that are classed as temporary are subject to PAT testing (Portable Appliance Testing) under the Electricity at Work Regulations 1989.
Information relating to the safe operation and use of projection equipment must be provided by the suppliers with all installations, especially in relation to beam viewing by teachers and pupils.

Board Heights

Concerns also exist with respect to the location of interactive whiteboards both from a teacher and a pupil perspective. If the board is too low the teacher may object to the positioning on the grounds of health and safety, conversely if the board is too high then pupils may not be able to reach the top portion of the board. If the latter is true then schools may choose to use a step or some staged area in front of the board which poses a significant trip/fall hazard.
There are currently no specific standards for the install height of an interactive whiteboard however there are several criteria that determine the most effective positioning of board:

1. To ensure compliance with health and safety requirements the projector should be mounted no lower than 2.2 metres from the floor.
2. The potential for image distortion (keystoning) when viewed from certain angles also determines at which point the interactive whiteboard can be positioned based on point

Schools should therefore undertake an appropriate risk assessment to ensure that the board is positioned at the most appropriate height for intended users.

14. Staff CPD

Staff development in ICT is ongoing within the school. It is our aim to raise the level of staff competence and confidence in ICT by:

- Giving teachers and support staff opportunities to attend INSET – to develop their knowledge and use of ICT across the curriculum
- Providing in–school support for teachers and support staff who require assistance in developing particular aspects of ICT skills knowledge and understanding
- Sharing good practice in the use of ICT
- Seeking opportunities for involvement in ICT-based projects within and beyond the school
- Participation in online learning

15. The Role of the ICT Co-ordinator/ICT Development Team

It is the responsibility of the ICT Co-ordinators along with the ICT Development Team to:

- Provide leadership and direction in ICT
- Ensure that the use of ICT is managed and organised to meet school aims and objectives
- Play a key role in school policy development in relation to ICT and teaching and learning
- Liaise with SMT in order to set priorities and targets to improve ICT provision
- Support, guide and motivate colleagues - which may require the provision of training for staff
- Contribute to the monitoring and evaluation process
- Keep up to date with recent developments in ICT and advise colleagues appropriately
- Ensure continuing personal professional development
- Model good practice by integrating ICT effectively into curriculum planning, classroom teaching and the assessment of children's work

16. The Responsibility of the Classroom Teacher

It is the responsibility of the classroom teacher to:

- Contribute to whole-school planning for ICT
- Integrate ICT into curriculum planning, classroom teaching and the assessment of children's work
- Ensure that any ICT resource/software used in the classroom is appropriate to curriculum needs and children's learning needs
- Ensure health and safety practices are carried out
- Discuss and devise with the children rules for using the computer
- Implement the e-Safety Policy

17. Management Information Systems (MIS)

ICT enables efficient and effective access to and storage of data for the school's management team, teachers and administrative staff. The school complies with SEELB requirements for the management of information in schools. We currently use SIMs which operates on the school's administrative network and is supported by C2K.

All teaching staff have read only access to Assessment Manager and the SENCO module. Only trained & designated members of staff have authority and access rights to input or alter the data. The school has defined roles & responsibilities to ensure data is well maintained, secure and that appropriate access is properly managed with appropriate training provided.

18. School Liaison, Transfer and Transition

The school is connected to the C2K intranet which enables the transfer of information electronically. Email is now used frequently to liaise with the SEELB, DENI, other schools and, where possible, parents. Future developments regarding our school management information system will enable the transfer electronically of data to aid transfer and transition to or between or within schools.

19. Legislation, Copyright and Data Protection

All software loaded on school computer systems must have been agreed with the designated person in the school. All our software is used in strict accordance with the licence agreement. We don't allow personal software to be loaded onto school computers. Please refer to the school's Data Protection Policy.

20. Environmental Impact of ICT

The school understands its obligation to look at the environmental impact of ICT and has taken steps to minimise it.

- Staff are continually encouraged not to leave equipment on standby and switch off the computers and printers each day
- A notice is displayed in the computer suite reminding teachers to ensure equipment is turned off
- The school has signed up to 'Recycool' which will recycle printer cartridges and, in the future, mobile phones, to raise funds for school ICT equipment
- Staff make greater use of internal email
- DENI, CCEA and SEELB and other external agencies mostly communicate via email so there is less paper correspondence
- C2K have set up scheduled tasks to run updates and shutdown computers

The disposal of equipment is dealt with by SEELB and therefore out of the control of the school.

21. E-Safety

Contents

Newtownards Model Primary School

Internet Policy

The Northern Ireland Revised Curriculum requires that pupils should be given opportunities to access and research information from safe and reliable sources. It also states that they should be allowed to '*communicate safely and responsibly….exchanging, sharing, collaborating and developing ideas digitally'*. It is also important that pupils can *'manage and present their work…..using ICT safely and responsibly'*. However, above all, pupils should be '*provided with opportunities to develop knowledge and understanding of e-safety and acceptable online behaviour'* and demonstrate this knowledge when and where appropriate. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable.

The Internet is an open communications channel, available to all. Applications such as the Web, e-mail and chat all transmit information over the wires and fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. Sadly e-mail and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Our Internet Policy has been written by the school, building on the SEELB and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Updated by:	E. McCulloch (ICT co-ordinator)
Date:	August 2016
Approved:	J. Stewart (Principal)

1.0 Core Principles of Internet Safety

The Internet is now as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing of pupils in embarrassing, inappropriate and even dangerous situations.

The Newtownards Model Primary School Internet Policy is built on the following five core principles:

Guided Educational Use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk Assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become "Internet Wise". We are fully aware of the risks, and so perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material.

Pupils may obtain Internet access in Youth Clubs, Libraries, and public access points and in homes. Ideally a similar approach to risk assessment and Internet safety would be taken in all these locations, although risks do vary with the situation.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

Regulation

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access within the school will be denied, for instance unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions.

Appropriate Strategies

This policy describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

2.0 School e-Safety Policy Questions

2.1 Who Will Write And Review The Policy?

- The school's ICT co-ordinator and Mr Stewart will review the policy.
- Our e-Safety Policy has been written by the ICT co-ordinator, building on the SEELB and government guidance. It has been agreed by the senior management and approved by governors.
- The e-Safety Policy will be reviewed annually.

2.2 Teaching And Learning

2.2.1 Why Is Internet Use Important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2.2 How Does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the SEELB, DENI and NI Curriculum; access to learning wherever and whenever convenient.

2.2.3 How Can Internet Use Enhance Learning?

- The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.2.4 How Will Pupils Learn How To Evaluate Internet Content?

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.3 Managing Information Services

2.3.1 How Will Information Systems Security Be Maintained?

- The security of the school information systems will be maintained by C2K.
- 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 Network solution.
- Access to the Internet via the C2k Education Network is fully auditable and reports are available to the school principal.
- Virus protection will be installed and updated regularly.
- Portable media may not used without specific permission and a virus check.
- Files held on the school's network will be regularly checked.
- The ICT co-ordinator will review system capacity regularly.

2.3.2 How Will e-Mail Be Managed?

- C2k recommend that all staff and pupils should be encouraged to use their C2k email system. It is strongly advised that staff should not use home email accounts for school business.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive 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.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- 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.

2.3.3 How Will Published Content Be Managed?

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

2.3.4 Can Pupil's Images Or Work Be Published?

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

2.3.5 How Will Social Networking And Personal Publishing Be Managed?

Social networking is everywhere. It is common to find parents, co-workers and others on such sites. With social networks, people across the world have access to tools and options that were previously non-existent. However, there are now just as many new opportunities to connect as there are to get into potential danger. One thing we often forget while having fun on social networks, is that almost anybody can see what we are doing. While we are tagging photos for our friends or are posting comments to them, it can be easy to forget that someone else who has been invited onto a social networking site can also view them.

Once something appears on the Internet, it is almost impossible to remove. As these sites continue to grow in popularity, so too does the value of the information on them to parties other than those directly involved. Social networking users need to take a step back and think about just what they are posting on to the Internet.

Guidelines for a Code of Conduct for those who work with children and young people.

The following guidelines should be read in conjunction with the school's Code of Conduct:

- People who work with children and young people should always maintain appropriate professional boundaries, avoid improper contact or relationships and respect their position of trust.

- With regard to relationships, individuals who work with children and young people should not attempt to establish an inappropriate relationship which might include:

    - communication of a personal nature

    - inappropriate dialogue through the internet

    - the sending of emails or text messages of an inappropriate nature

- Individuals who work with children and young people should be extremely careful in corresponding with people on social networking sites
- Staff relationships with children and young people should at all times remain professional and they **must** not correspond with children and young people through such sites or add them as 'friends'
- It is worth bearing in mind that on such sites inappropriate or even misconstrued communication may have the potential to impact upon their careers or even result in a criminal investigation
- Staff should bear in mind who may access their own profiles on such websites and should therefore take care as to the information they display about themselves and their personal lives. They should also ensure that they have installed and are using the appropriate privacy settings.
- Individuals who work with children and young people should not make, view or access illegal or inappropriate images of children.

- Individuals who work with children and young people and others, with whom they may be in a position of trust, should exercise caution when using social networking sites and avoid inappropriate communication of any kind.

Pupils and Social Networking Sites

- C2K block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- 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.
- Schools should also keep good records of cyber-bullying incidents to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

2.3.6 How Will Filtering Be Managed?

- The school will work in partnership with C2K and Northgate to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the internet service provider via the ICT co-ordinator.

2.3.7 How Will Video Conferencing Be Managed?

The equipment and network

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school web site.
- The equipment must be secure and if necessary locked away when not in use.

- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.
- Parents and Guardians should agree for their children to take part in videoconferences, probably in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the videoconferencing system web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

2.3.8 How Can Emerging Technologies Be Managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils should be aware that mobile phones and electronic devices with camera and Wi-Fi facilities are banned from school.
- The school should investigate cellular wireless, infra-red and Bluetooth communication.
- Pupils are not permitted to bring their mobile phone into school.
- Staff will be issued with a school phone where contact with pupils is required.

2.3.9 How Should Personal Data Be Protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 How Will Internet Access Be Authorised?

- The school will maintain a record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'The Acceptable Use Agreement' before using any school ICT resource.
- Access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

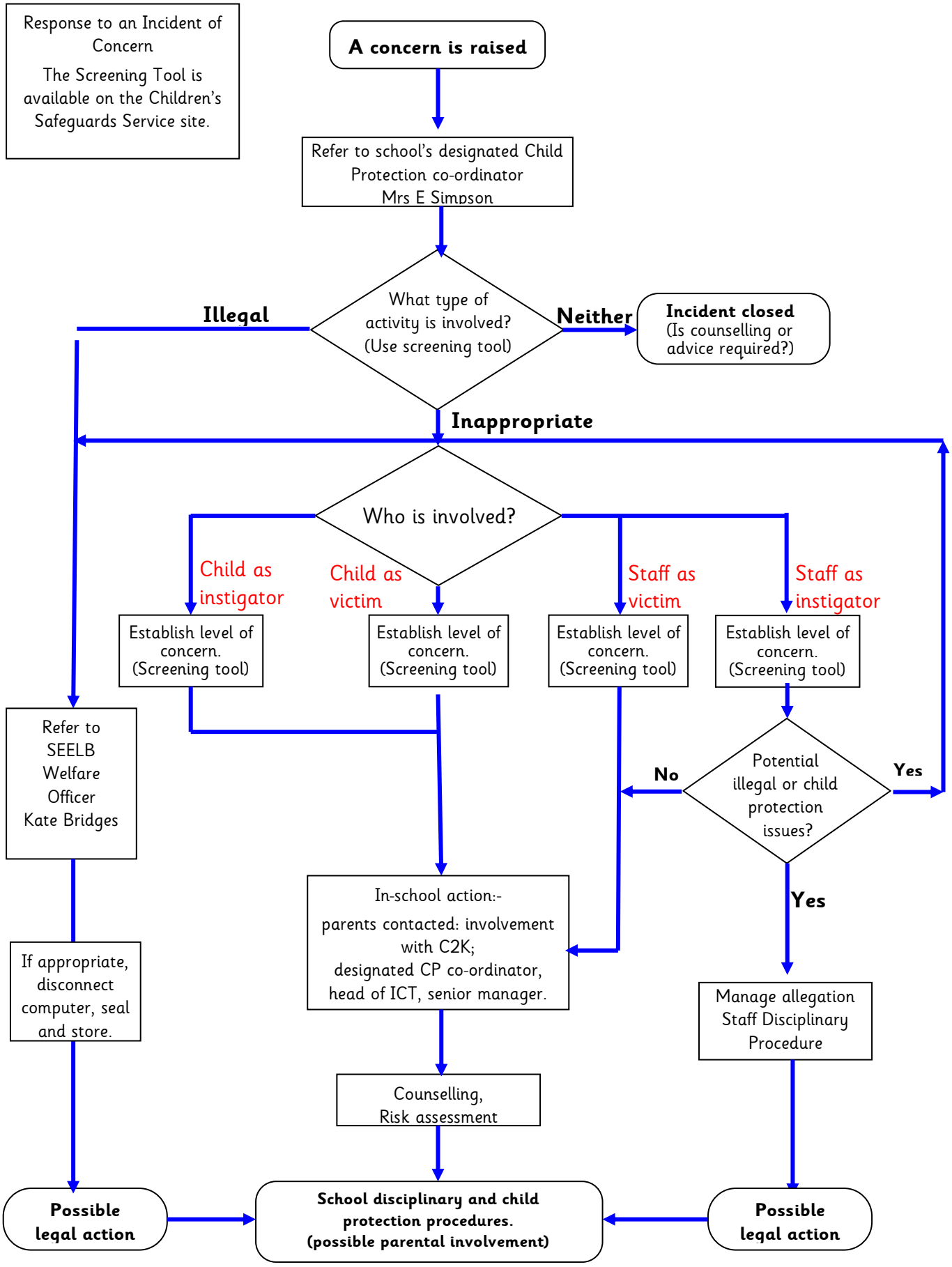
2.4.2 How Will Risks Be Assessed?

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".

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor C2K can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Risk assessments will be carried out on the technologies within school to mitigate against the potential risks involved with their use.
- The school risk assessments will inform the teaching and learning, develop best practice and be referenced in the school's Acceptable Use Policy.
- Methods to identify, assess and minimise risks will be reviewed regularly
- The principal will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

2.4.3 How Will e-Safety Complaints Be Handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Principal. Any complaint about Principal misuse must be referred to the Vice-Principal or Chair of Governors.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions will be linked to the School's Behaviour Policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator.
- Should anyone be concerned about the Internet usage of a pupil or member of staff, the flowchart on the next page should be used as guidance. It is taken from the Children's Safeguards Service website and illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Children's Safeguards Service has provided supporting documents to assist school's when responding to incidents.
- See Screening tool - Appendix A


Response to an Incident of Concern
The Screening Tool is available on the Children's Safeguards Service site.
A concern is raised
Refer to school's designated Child Protection co-ordinator Mrs E Simpson
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Refer to SEELB Welfare Officer Kate Bridges
Potential illegal or child protection issues?
No
Yes
Yes
In-school action:- parents contacted: involvement with C2K; designated CP co-ordinator, head of ICT, senior manager.
If appropriate, disconnect computer, seal and store.
Manage allegation Staff Disciplinary Procedure
Counselling, Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action

2.4.4 How Is The Internet Used Across The Community?

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

2.5 Communications Policy

2.5.1 How Will The Policy Be Introduced To Pupils?

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Internet Safety is incorporated into the PDMU Scheme
- Pupils will be given a general internet safety talk as part of the school's 'Internet Safety Week'
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be included in the ICT Scheme of Work, covering both school and home use.

2.5.2 How Will The Policy Be Discussed With Staff?

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff development in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

2.5.3 How Will Parents' Support Be Enlisted?

- Parents' attention will be drawn to the School E-Safety Policy in Data Capture Form and on the school website.
- Internet issues will be handled sensitively to inform parents without alarm.
- A partnership approach with parents will be encouraged. A parent's afternoon has been arranged with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in section 4.0 e-Safety Contacts and References.

Rules for Responsible Internet Use

These rules help us stay safe!

- ✔ I will only log on using my own username and password, which is a secret.
- ✔ I will ask permission before going on an Internet site.
- ✔ I will only e-mail people I know or my teacher has approved.
- ✔ I will only send messages which are polite and sensible.
- ✔ I will not give out my home address or telephone number or arrange to meet anyone.
- ✔ I will not use Internet chat.
- ✔ I will tell a teacher if I see anything which I am unhappy with.
- ✔ I will not interfere with anyone else's work.
- ✔ I will not damage computers or other equipment.
- ✔ I will not download or install any programs on any school computer.
- ✔ I understand that the school may check my files and what I have been looking at on the Internet.

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

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

The Acceptable Use Policy: All Adults Working In School

For Personal Use:

Do not give anyone access to your login name or password.

Do not open other people's files without express permission. Do not corrupt, interfere with or destroy any other user's information.

Do not release personal details including phone numbers, fax numbers or personal e-mail addresses of any colleague or pupil over the Internet.

Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.

Do not attempt to visit sites which might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden.

Users should log out and close their browser when their session has finished.

Personal E-mail

Follow school guidelines contained in the ICT policy for the use of e-mail.

Observe *netiquette* on all occasions. E-mail should not be considered a private medium of communication.

Do not include offensive or abusive language in your messages or any language which could be considered defamatory obscene, menacing or illegal. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority. You should be aware that C2K e-mail is automatically monitored.

Make sure nothing in the messages could be interpreted as libellous.

Do not send any message which is likely to cause annoyance, inconvenience or needless anxiety.

Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

When Using The Internet, Learning Platform Or e-Mail With Children

Remind children of the rules for using the Internet and e-mail.

Watch for accidental access to inappropriate materials and report the offending site to the ICT co-ordinator, who will report it to C2K.

Report any breaches of the school's Internet policy to the ICT co-ordinator or Principal.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

The Acceptable Use Policy: All Adults Working In School

Please sign and date if you have read and understood the:-

- E-Safety Policy

Print Name	Signature	Date	Print Name	Signature	Date
Mr Stewart			Mrs Thompson		
Mrs Gould			Mrs Ringland		
Mrs Langley			Mrs Leathem		
Mrs Hopkins			Mrs Wilkinson		
Mrs Ryan			Mrs Hill		
Mrs McCulloch			Mrs King		
Miss Beattie			Mrs Boyd		
Miss Cooper			Ms Fulton		
Mr Watson			Mrs Dines		
Miss Owens			Miss Donnelly		
Mrs Lyttle			Mrs McBride		
Mr McCullough			Mrs Webber		
Mrs Myles			Mrs McFeeters		
Mrs Simpson			Mrs Dornan		
Mrs Turtle			Mr Rollo		
Mrs Braniff					
Mrs Templeton					

4.0 e-Safety Contacts and References

e-Safety in Schools and Schools e-Safety Policy	http://www.clusterweb.org.uk?esafety
Schools e-Safety Blog	http://clusterweb.org.uk?esafetyblog
Child Exploitation & Online Protection Centre	http://www.ceop.gov.uk/contact_us.html www.thinkuknow.co.uk
Virtual Global Taskforce – Report Abuse	http://www.virtualglobaltaskforce.com/
Think U Know website	http://www.thinkuknow.co.uk/
Becta	http://www.becta.org.uk/schools/esafety
Internet Watch Foundation	http://www.iwf.org.uk/
Internet Safety Zone	http://www.internetsafetyzone.com/
Staying SMART Online	http://www.kidsmart.org.uk/
NSPCC	http://www.nspcc.org.uk/html/home/
Childnet International	www.childnet.com needadvice/needadvice.htm
Childline	http://www.childline.org.uk/
Stop Text Bully	www.stoptextbully.com
Bullying Online	www.bullying.co.uk
NCH – The Children's Charity	http://www.nch.org.uk/stories/index.php?i=324
NCH – Digital Manifesto	http://www.nch.org.uk/uploads/documents /Digital_Manifesto_web.pdf
BBC Chat Guide	http://www.bbc.co.uk/chatguide/
CBBC – Stay safe	http://www.cybersmartkids.co.au
Childnet International	www.childnet-int.org
Hector's World TM	www.hectorsworld.com
NetSmartzKids	www.netsmartzkids.org
PHONEbrain	www.phonebrain.org.uk
Safe Surfing with Doug	www.disney.co.uk/DisneyOnline/safesurfing
Surf Swell Island: Adventures in Internet Safety	www.disney.go.com/surfswell
Netty's World	www.nettysworld.com.au
For Kids by Kids Online	www.fkbko.co.uk
iKeepSafe.org	www.ikeepsafe.org

5.0 Notes On The Legal Framework

An awareness of legal issues is important, but this page is not definitive advice.

Many young people and indeed some staff use the internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes include:

- The 2003 Sexual offences Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18.
- Offences regarding racial hatred are covered by the Public Order Act 1986 although a new Racial and religious Hatred Bill is going through parliament.

5.1 Possible Offences:

Sexual Offences Act 2003

- Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
- Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image.)
- Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.
- Abuse of positions of trust - Staff must be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Applies to teachers, social workers, health professionals, ancillary staff)

N.B. Schools should already have a copy of 'Children & Families: Safer from Sexual Crime' document as part of their child protection packs. Information about the 2003 Sexual Offences Act can be found at ww.teachernet.gov.uk

5.2 Relevant Legislation

The Computer Misuse Act 1990

- makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Public Order Act 1986

- offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Communications Act 2003

There are 2 separate offences under this act:

a) sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.

b) sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

This wording is important because the offence under a. is complete when the message has been sent - no need to prove any intent or purpose. It is an offence under b. to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.

Malicious Communications Act 1988

- offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.

Data Protection Act 1984/98

- concerns date on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988

- it is an offence to use unlicensed software.

Protection of Children Act 1978

- the law on images of child abuse is clear. It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.

Obscene Publications Act 1959 and 1964

- defines 'obscene' and related offences.

Protection from Harassment Act 1997

Section 2 - A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Section 4 - A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of hose occasions.

5.3 Monitoring School ICT Use

Monitoring network activity could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998.

The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of the network, but then allow private use following application to the principal. The Rules for Responsible Internet Use, with which every user agrees to comply, contains a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

5.4 Sex Offences Act 2003 Memorandum of Understanding

Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003.

The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences so that they will be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse. This memorandum has been created within the context of child protection, which will always take primacy.

The MOU: http://www.iwf.org.uk/police/page.22.213.htm

APPENDIX A

Screening Tool

This screening tool can be used to assist decision making in dealing with incidents of computer or e-communications misuse within your school. It can be used to inform initial action but is not a substitute for a thorough risk assessment / investigation.
This should be used alongside the e-Safety flow chart and incidents of misuse matrix.

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact Kate Bridge (EWO) at SEELB - 028 9056 6200 ext: 6900.

Also use: http://www.clusterweb.org.uk ?safeguards

Type of incident

- Sexual ☐
- Bullying ☐
- Violence ☐
- Incitement ☐
- Financial ☐
- Grooming ☐
- Other ☐

How was the incident discovered?

- Self reported ☐
- Reported by 3rd party (friends or parents) ☐
- Reported by Teacher ☐
- Other (e.g. Police or Internet Watch foundation) ☐

What was their response to the incident?

- Unconcerned ☐
- Curious ☐
- Distressed ☐
- Frightened ☐
- Secretive ☐
- Other ☐

What did the incident refer to?

Answer the key questions relating to the particular incident.

Child as Instigator:

Content

Refer to 'Child as Victim' questions on content.
Refer to AIM project matrix to assess the child's response to the content.

Incitement

1. Was the child secretive about the site?
2. Did the child access the site in an isolated place?
3. Did they understand the risks of accessing this site?
4. Was their response to the site…
    - Healthy (e.g. using for research)
    - Problematic (looking for advice or guidance)
    - Harmful (relying on site for tips, using site to communicate with likeminded individuals, the site is reinforcing /minimising potentially harmful behaviours e.g. self-harm, pro anorexia sites

Send/Publishing

1. Has an offence taken place?
   (refer to glossary for information on what constitutes an offence)
2. Were others put at risk e.g. their image / information was sent / published
3. Was this an isolated incident or persistent?
4. Did the instigatator have empathy for the victim?

Interception of communications / Hacking

1. Have they placed themselves or others at risk?
2. Has personal or financial information been stolen?
   (If yes, this constitutes a criminal offence and advice should be sought from the police)
3. Has illegal content been accessed and sent to other's computers?

N.B. The 'AIM project' matrix for assessing appropriate child behaviour can also be referred to in this instance where the child has instigated the behaviour.
Although developed to help understand sexualised behaviour the AIM matrix may be helpful in understanding other situations where there is a perpetrator/victim relationship"

Once you have gathered the appropriate information, assess the effect of the incident on the child and identify how the child can be best supported. This may be either in school (using the Pastoral Care Policy and resources to support children) or in certain circumstances with external help (Police, Kate Bridges, etc)

Child as Victim:

Content

1. What was the type of content? (Sexual, violence, racial, other)
2. Did anyone else see it?
3. Have they told anyone else about it?

Publishing

1. Is the child identifiable?
2. Can their location be traced?
3. Is text or image potentially indecent or illegal?

Bullying

1. What was the type of bullying? (sexual, violent, physical, group)
2. Were information or images published of the child?
   (If yes, refer back to publishing section for more questions to ask)

Predation / Grooming

1. Assess the extent of the contact
   - One off conversation
   - Regular conversation
   - Regular conversation using inappropriate or sexualised language or threats
   - Attempts to breakaway
   - Offline meeting arranged
   - Offline meeting occurred
     (Consider if an offence has occurred)
2. Are the parents aware?
3. When did the incident occur?

Request for information

1. Did the child give out any personal information?

Staff misuse:

- Did the member of staff misuse the school's internal email system?
- Did the member of staff communicate with a young person inappropriately e.g. via text message, multimedia images.
- Consider the extent of the communication
  - One off conversation
  - Regular conversation
  - Regular conversation using inappropriate or sexualised
    - language or threats
  - Attempts to breakaway
  - Offline meeting arranged
  - Offline meeting occurred
    - (Consider if an offence has occurred)
- Did the member of staff access inappropriate / illegal material within school?
- Did the member of staff access inappropriate / illegal material using school equipment?
- Did the member of staff access inappropriate / illegal material using their own equipment?

APPENDIX B

AIM Project Matrix: Checklist for Understanding Sexualised Behaviour

	Healthy	Problematic	Harmful
1. Type of Sexual Behaviour	Age appropriate, mutual and exploratory	Not age appropriate or has some knowledge or language	Adult sexually activity e.g. intercourse, oral sex etc
2. Context of behaviour	Open, light hearted, spontaneous	No secrecy or force, but children involved seem uncomfortable	Behaviour is planned, secretive; there are elements of threat, force, and coercion. The children targeted seem anxious, fearful, and uncomfortable.
3. Response of other children	Engaging freely, happy	Uncomfortable, unhappy with behaviour but not fearful or anxious. If directed at adults they feel uncomfortable	Uncomfortable, unhappy, fearful, anxious. Could be physically hurt. Could be trying to avoid the other child
4. Relationship between the children	Similar age and ability would normally play together. There are no factors to suggest a power imbalance	Children would not normally play together or there may be factors which suggest one child is more in control than the other	Children would not normally play together or there are clear power differences e.g. due to age, size, status, ability, strength
5. Frequency of behaviour	Behaviour is age appropriate, ad hoc and not the main focus for the child. The child is interested in other things	Some inappropriate sexual behaviour for age, however child also has interest in other things, behaviour is intermittent	Frequent incidents and child seems focussed on behaviour. It is disproportionate to other aspects of their life. They seem to seek comfort / reassurance / or control from the behaviour
6. Persistence of behaviour	Behaviour is age appropriate, ad hoc and not the main focus for the child. The child is interested in other things	Behaviour is recurring and there are some difficulties in distracting and redirecting behaviour. Child however is responsive to some intervention	Child cannot be distracted from the behaviour easily and returns to the behaviour Focus on the behaviour is disproportionate to other aspects of their life It appears to be the main way they seek comfort / attention and control
7. Child's emotional response	Happy, embarrassed, able to take responsibility for their behaviour and its effects on others (dependant on their age & understanding)	Child unresponsive, ashamed, struggles to take responsibility for their behaviour or to show empathy	Child angry, fearful, aggressive, distressed or conversely passive, lacking in understanding why anyone would be worried Cannot take responsibility for their behaviour, nor shows any empathy for others
8. Background information	Nothing known of concern	Little known about the family or there are some concerns about the family. There are concerns about other difficult behaviours	Patterns of discontinuity of care / poor attachments High levels of trauma e.g. physical, emotional, sexual, neglect, domestic violence Other behavioural problems or conduct disorder