



BALLYCASTLE HIGH SCHOOL

ICT and Acceptable Use of the Internet Policy

- *Approval by the Board of Governors: **29 September 2015***
- *The implementation of this policy will be monitored by: Senior Management Team*
- *This policy will be reviewed annually*



I.C.T. POLICY INCLUDING DATA SECURITY AND ACCEPTABLE USE OF THE INTERNET

Ballycastle High School believes that:

- ICT literacy is a key skill in developing pupil learning and is becoming as important as literacy in language and application of number. Therefore the ability of pupils to effectively use ICT to deepen and develop their learning is of utmost importance.
- ICT can encourage pupils to become more independent in their own learning by developing their skills in finding and using appropriate information. This in turn can help develop skills that will contribute to the life-long learning of pupils.
- ICT can provide access to sources of information beyond the normal scope of the school.
- All pupils are entitled to access to computers where this will further or deepen their learning and understanding.

It is the aim of the school:

- To develop and extend the individual ICT skills of all pupils.
- To use ICT skills learned through ICT classes to enhance, enrich and extend learning in other curriculum subjects.
To encourage pupils to recognise and be confident with the appropriate uses of ICT.
- To increase pupil motivation and self-esteem by improving the presentation of their work.
- To use ICT, when appropriate, to improve the learning experiences of all pupils.

The School seeks to achieve these aims through developing:

- Pupil knowledge and understanding of ICT technology used to promote their ICT skills so that they are at a level appropriate to their age and ability.
- Links across the curriculum subjects so that pupils can not only further their knowledge of ICT skills but also deepen their knowledge of other areas of study.
- Pupil understanding of the benefits of using ICT both in the school environment and the wider world.



STAFF

All staff use ICT regularly in the course of their normal duties. The following staff have particular responsibilities with regards to certain areas of ICT provision.

The Principal is responsible for the purchase of ICT equipment throughout the school, for the implementation of the ICT Policy and in conjunction with the Head of ICT, for Key Stage 3 ICT Assessment and staff development in the use of ICT.

The C2K Manager is responsible for liaising with C2K on ICT related issues and ensuring that staff are kept up to date with changes to and trained in the use of the C2K managed services.

The Head of ICT is responsible for the curricular provision of ICT in school and, in conjunction with the Senior Teacher with Responsibility for ICT for Key Stage 3 ICT Assessment and staff development in the use of ICT.

ICT Subject Leaders, work with the Head of ICT to co-ordinate Key Stage 3 ICT Assessment. They work within departments to encourage the consistent use of ICT and further develop staff ICT skills.

The ICT Technician is responsible the smooth running of the school networks and related hardware and software. They work closely with the Senior Teacher with Responsibility for ICT and the Head of ICT.

PROMOTING THE SUBJECT WITHIN THE SCHOOL / CROSS-CURRICULAR THEMES:

ICT is promoted as a cross curricular theme in the school. All subject areas are required to include ICT in their curriculum materials and schemes of work. Each department has been surveyed to ascertain the current position of ICT provision in the relevant schemes of work. This procedure is carried out periodically to assess the development of ICT provision in the school.

Each Head of Department has been made aware of his or her responsibility with regard to ICT provision in the curriculum of their subject and support has been offered to departments where necessary.

This support has included the providing each department with sample ICT assignments as suggested by CCEA. These assignments are subject based and provide Teacher and Pupil notes on the purpose of the assignment and how to carry it out. Departments were encouraged to use these assignments where no ICT assignments were included in schemes of work. Staff training is also provided to introduce new network procedures or how to use software and hardware as appropriate.



Each department should include an ICT based assignment as a benchmark assignment for each year group and the implementation of this strategy would help meet the requirement of ICT provision in subject areas.

ICT IN THE SCHOOL CURRICULUM

At present there exists a statutory requirement on schools in Northern Ireland to 'provide pupils with opportunities to develop knowledge, skills and understanding of Information and Communication Technology (ICT) and to apply these in a range of subjects.'¹ Currently in Northern Ireland there is no provision at Key Stage 3 for ICT to be taught as a specific subject, instead it is intended that ICT be included in the curriculum as a cross-curricular theme.

With these requirements in mind each subject area in the School has been encouraged to build ICT into their Programmes of Study. This should take the form of at least one ICT based assignment in the Scheme of Work for each year group. It is intended that, across the whole school curriculum, these assignments will address the 5 'E' requirements (explore, express, exchange, evaluate and exhibit) and each of the 7 levels.

Alongside this cross-curricular approach, ICT is taught as a discrete subject in Years 8 and 9. The rationale behind this approach is that the timetabled ICT classes provide pupils with the opportunities to learn and develop the skills necessary to operate the computers and use the various software packages available. This means that a subject teacher should not have to use valuable teaching time showing a class how to use a particular piece of equipment or a software package. This means that the time pupils spend using the computers is focused on completing the task at hand rather than learning ICT skills.

ASSESSMENT PROCEDURES

The Northern Ireland (Revised) Curriculum places a requirement on schools to assess and report on progress in the cross curricular skill of Use of ICT. A department has been given the task of reporting on this skill in each year group in Key Stage 3. Two departments in each year group are to be asked to assess progress through the levels once these levels are agreed.

¹ 'Teacher's Handbook – Accreditation of Information Technology Assessment', produced by CCEA 1997 ISBN 1 85678 949 7 – p.3



SPECIAL EDUCATIONAL NEEDS

Visual Impairment

The literacy and numeracy problems experienced by visually impaired people are likely to include:

- a lack of reading, writing and numeracy practice
- difficulty in scanning pages or even in scanning words

Computers are used to provide alternative methods of reading and recording work. The high contrast print is easier for pupils to see than handwriting and pupils who need to use large print on a computer screen. Podcasting is used as an alternative means of providing information.

Hearing Impairment

ICT can be of particular benefit to people with a hearing impairment because it allows them opportunity to extend their language skills by use of pictures, text etc. without being dependent on the spoken word.

Dyslexia

ICT can motivate learners with dyslexia to acquire skills for reading, spelling, writing and maths. Word processors with spell checkers, glossaries and thesauri can all help pupils master literacy skills as they aid punctuation, encourage word recognition and help pupils to extend their vocabulary by enabling them to use the words they want to use rather than the ones they can spell.

EQUIPMENT AND RESOURCES

The school has the following ICT resources available for teaching ICT
 Across the school we have a whole school network of 105 PC's (C2K network PC's). These PC's have a large number of software packages that can be allocated for pupil and staff use. The network is connected to the internet via a broadband connection. The school makes use of the c2k Meru wifi system.

- Room 13 – 24 PC's, B&W Laser printer, Colour laser, data projector
- Room 22 – 24 PC's, B&W Laser printer, data projector
- Room 25 – 24 PC's, B&W Laser printer, data projector
- Technology 18 PC's, B&W Laser printer, data projector, Laser cutter
- Library – 5 PC's, B & W Laser, Colour printer
- Art has a cluster of 4 PC's with access to an A3 scanner
- HE has a cluster of 14 PC's in the resource room
- There is a laptop trolley with 20 laptops.
- The remaining C2K PC's are spread throughout the school, many as teacher workstations and also in the 6th Form study to support learning.
- ICT & Media has a separate suite of Apple Macs in Rm 8.



There are additional iMacs available in Rm. 15, library, 6th Form study and staffroom.

All teaching staff have iPads for the support of teaching and learning. There are a small number available for pupils with Special Educational Needs. iPad apps and usage are monitored using the Meraki system.

There is a separate wifi network throughout the school for this purpose. Access is strictly controlled. Internet access is filtered using a Draytek system with similar filters in place as the c2k system.

All classrooms have interactive boards and Apple TV systems

Resources are maintained and replaced as required through the provision of:

- An annual budget allocated from the school. This budget is for the following purposes:
 - Purchase of ICT equipment to replace stock and upgrade equipment as and when necessary.
 - General maintenance of the ICT facilities including repairs and replacement of hardware when necessary.
 - Purchase of consumables for the general running of the ICT suites including paper, ink and toner, etc.
 - Purchase of additional hardware requested by departments or for whole school use.
 - Purchase of additional software packages to aid teaching of ICT or other subject areas.

E SAFETY

– safeguarding children and young people in the digital world.

Please see the full policy on E-Safety.



DATA SECURITY

The Data Protection Act (DPA) requires organisations to have appropriate technical and organisational measures in place when storing and sharing personal data. Organisations must protect information they hold themselves and establish appropriate security in respect of sharing information.

Computer security is constantly evolving, and is a complex technical area. Technical security measures to protect computerised information are of obvious importance. However, many security incidents relate to the theft or loss of equipment, or to old computers or hard-copy records being abandoned. Physical security includes things like the quality of doors and locks, and whether premises are protected by alarms, security lighting or CCTV. It also includes control of access to premises, supervision visitors, disposal of paper waste, and keeping portable equipment secure.

Personal data is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining, or disposing of information. The data protection principles apply to all information held electronically or in structured files that tells you something about an identifiable living individual. The principles also extend to all information in education records. Examples would be names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

Sensitive personal data is information that relates to race and ethnicity, political opinions, religious beliefs, membership of trade unions, physical or mental health, sexuality and criminal offences. The difference between processing personal data and sensitive personal data is that there are greater legal restrictions on the latter.

Electronic personal data

Strong passwords, i.e. at least eight characters long and containing special symbols, should be used if any electronic equipment holds confidential personal information. There are regular prompts to change passwords and use different passwords for separate systems and devices. Encryption software should be used to protect all portable devices and removable media, such as laptops and USB devices (or another form of memory storage not part of the computer itself), which hold confidential personal information. This is particularly important if they are taken from school premises. It is also important to prevent access to the information in case equipment is stolen. Memory sticks are easily lost, and laptops are attractive to thieves.



Computer security

- Staff profiles only allow access to the information they need to do their job.
- Workstations only allow access as appropriate to their location.
- Regular back-ups of the information on the computer system are taken and kept separately.
- All personal information is securely removed before disposal of old computers (by using technology or destroying the hard disk).

Email security protocol for all staff

- Give consideration as to whether the content of the email should be encrypted or password protected.
- When starting to type in the name of the recipient, some email software will suggest similar addresses you have used before. Previously emailed people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure the right address is chosen before you click send.
- It is possible to send an email to a recipient without revealing their address to other recipients, make sure to use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.
- If personal or sensitive personal data is being sent as an attachment it should be password protected, and where feasible, be anonymised.
- Messages within school containing Personal or Sensitive Personal data should be sent using the SIMS messaging system

Data Security Breach-Management

Breach management will follow the principles:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.
2. Assessing the risks – assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, assess the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.



3. Notification of breaches – informing people about an information security breach can be an important part of managing the incident, but it is not an end in itself. Consider notifying the individuals concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.
4. Evaluation and response – it is important to investigate the causes of the breach and also evaluate the effectiveness of the response to it. If necessary, update your policies and procedures accordingly.

School staff should inform the ICT Manager immediately the breach is discovered.



EQUIPMENT AND NETWORK SECURITY

1.1. Virus Check and Firewall

C2K PC's

All of the C2K PC's in school are maintained under the C2K maintenance contract and are administered as part of the C2K WAN service for Northern Ireland. This means that these machines are automatically protected by both anti-virus software and by firewall software as this is provided by C2K.

1.2. Password Security

C2K PC's

On entrance to the school new staff and pupils are provided with an initial password for the C2K system as provided by C2K. On their first attempt to log onto the network users are prompted to change their password to a password of their choice. These passwords must be at least 8 characters long. Once a term all users are required by the C2K system to change their password and each new password must be unique and the same password cannot be reused. Users may change their own password at any time if they feel that their password security has been compromised this can be done by the user themselves or by contacting one of the Network Administrators in school.

1.2.1. Portable School ICT Equipment, e.g. Laptops, Data Projectors, etc.

School laptops should be brought into school (at least once a week) to be connected to the C2K system. This is necessary to ensure that the network software and anti-virus protection is kept up to date. Software should not be installed on the school laptops unless the user has a valid license for the software. Users should also note that only school related software packages should be installed on the laptops to conserve disk space.

Equipment located in departments is to be used under the direction of the Head of Department and according to recognised user instructions.

Centralised equipment held in the ICT Administrator's office is to be borrowed for school use only and is recorded by the C2K Administrator in their Daily Diary (located in the Administrator's office).



HEALTH AND SAFETY

Due regard is paid to health and safety regulations and fire/emergency procedures are clearly posted. Pupils are instructed about the necessary safety standards when using the PC suites, for example, no eating or drinking in the suites, no running, how to sit properly, taking breaks, etc. Safety also takes into consideration the Internet and pupils are given advice and instructions on how they should use the Internet safely. Parents/Pupils also sign an Acceptable Use Policy which outlines safe use of the PC's in school and access to communication technologies.

Pupils are fully briefed on e-safety in Year 8 by their Registration teacher, and this is reinforced in Year 9 ICT lessons. In addition, the Child Protection Officer provides an additional briefing.

STAFF DEVELOPMENT

As ICT is a continually changing aspect of school life, the school aims to encourage and support staff to keep themselves up-to-date with developments in their subject area. The school provides internal training opportunities and encourages staff to avail of external training opportunities such as:

- EA ICT training and ICT subject training
- Private/ in house training workshops

LEGAL CONSTRAINTS

All users are expected to comply with the provisions of the following Acts of Parliament (or any re-enactment thereof) as well as all other relevant legislation and legal precedent:

Computer Misuse Act 1990
 Criminal Justice and Public Order Act 1994
 Copyright, Designs and Patents Act 1988
 Trade Marks Act 1994
 Data Protection Act 1998

Copies of these documents are available online at <http://www.opsi.gov.uk/>. Further advice should be obtained through the C2K Manager.

Note

ICT is by its nature an ever changing area. As such, this policy is regularly updated and should be considered as a work in progress. Updated policies will be forwarded to all interested parties as and when appropriate.



WHOLE SCHOOL POLICY ON ACCEPTABLE USE OF THE INTERNET, VLE AND DIGITAL IMAGES

What is the Internet and VLE?

The Internet is an electronic information highway connecting many thousands of computers all over the world and millions of individual subscribers. This global "network of networks" is not governed by any entity. This means that there are no limits or checks on the kind of information that is maintained by, and accessible to, Internet and VLE users. The educational value of appropriate use of information and resources located on the Internet and VLE is substantial.

A Virtual Learning Environment (VLE) is a range of educational resources, comprising information, forums, quizzes and other online material provided to students as part of an online learning package.

Rationale for pupil use of the Internet and VLE

Ballycastle High School encourages use by pupils of the rich information sources available on the Internet and VLE, together with the development of appropriate skills to analyse and evaluate such resources. On-line resources offer a broader range of up-to-date resources to pupils; provide an independent research facility; facilitate a variety of learning styles and abilities and encourage students to take responsibility for their own learning. Internet and VLE and e-mail literacy are fundamental requirements for all pupils as preparation for the Information Age – an era where ICT is a dominant factor in work and home life.

Networked Access to Internet and VLE

In recognition of these benefits, the school in conjunction with C2K NI has invested in providing networked Internet and VLE Access to pupils free of charge, and is determined to provide high quality training for staff and pupils to make best use of these facilities. Pupils will be provided with appropriate training and guidance on how to use the Internet during ICT classes. Appropriate cross-curricular use of the Internet and VLE is encouraged.

How will pupils gain access the Internet and VLE at Ballycastle High School?

- In ICT lessons
- Through subject use across the curriculum
- In the Sixth Form, during normal school hours and lunch-times for specified research purposes with the permission of a teacher



School website

The school website is intended to:

- provide accurate, up-to-date information about our school;
- enable pupils to publish work for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
- celebrate good work;
- provide pupils with the opportunity to publish their work on the internet;
- promote the school.

Parental permission will be needed before children's work can be published on the Internet. All classes may provide work for publication on the school web site and class teachers will be responsible for ensuring that the content of the pupils' work is accurate and that quality of presentation is maintained.

The points of contact on the web site will be the school address, telephone number and e-mail address.

Home information or individual e-mail identities will not be published. Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

Are there any dangers in using the Internet and VLE?

Since the Internet and VLE is composed of information from a vast array of sources world-wide, it includes some material that is not of educational value in the context of the school. This material includes information that may be inaccurate, abusive, profane, sexually oriented, racist or illegal. In order to guard young people from any inherent dangers, it is the joint responsibility of school staff and the parent or guardian of each pupil to educate the pupil about his or her responsibility when using the Internet and VLE. The following policy sets out the policy for acceptable use of the Internet and VLE at Ballycastle High School.

Promoting Safe Working Practices

During ICT lessons pupils will be advised of the Health and Safety issues surrounding the use of computer technology.

The guidance will focus on

- Posture and Seating
- Lighting
- Electrical Safety
- Keyboard Health and Safety
- Creating a Safe Working Environment

In addition, all staff will be made aware of Health and Safety requirements and receive a specific Health and Safety briefing.



Promoting Awareness with Parent, Governor and Community

Ballycastle High School is committed to ensuring all stakeholders are made aware of the Acceptable Use Policy. The policy will be:

- Disseminated to new parents
- Disseminated to new governors
- Available on the school web site



ACCEPTABLE USE OF THE INTERNET AND VLE

1. Pupils

a) Pupils are responsible for good behaviour on the Internet and VLE just as they are in the classroom or a school corridor. General school rules apply. In addition, a number of rules relating to use of the Internet and VLE also apply. An acceptable use policy is made available to all computer users at Ballycastle High school.

b) Ballycastle High has implemented a filtered Internet and VLE service through C2K NI and a filtered e-mail service (as recommended by UK government) through C2K NI. Pupils are **not permitted** to use any other e-mail service during use of the Internet and VLE in school. **Internet and VLE and e-mail services are monitored and are not therefore private – Internet and VLE activity and e-mail messages can be viewed at any time.**

c) Students at Ballycastle High should **know and understand** that no Internet and VLE user is permitted to:

- retrieve, send, copy or display offensive messages or pictures;
- use obscene or racist language;
- harass, insult, bully or attack others;
- damage computers, computer systems or computer networks;
- violate copyright laws;
- use another user's password;
- trespass in another user's folders, work or files;
- intentionally waste resources (such as on-line time and consumables);
- use the network for unapproved commercial purposes.
- Use ICT resources in any way that contravenes Health and Safety guidelines

d) Access to the Internet and VLE requires parental permission and a signed declaration by pupils agreeing to the school rules for use of the Internet and VLE.

e) Ballycastle High School will ensure that all pupils understand how they are to use the Internet and VLE appropriately and why the rules exist. Pupils will be directed to the pupil version of this policy on first using the Internet and VLE, and during subsequent sessions as changes are made/issues arise.

f) The Internet and VLE is provided for pupils to conduct research and communicate with others. While the use of information and communication technologies is a required aspect of the statutory Northern Ireland Curriculum, access to the Internet and VLE and C2K NI remains **a privilege and not a right**. It is given to pupils who act in a considerate and responsible manner, and will be withdrawn if they fail to maintain acceptable standards of use.



g) During school hours teachers will guide pupils towards appropriate materials. Outside school hours, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio, and other potentially offensive media.

h) When using the Internet and VLE at Ballycastle High School, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws.



2. Examples of Acceptable and Unacceptable Use

a. On-line activities which are encouraged include, for example:

- the appropriate use of email and computer conferencing for communication between colleagues, between pupil(s) and teacher(s), between pupil(s) and pupil(s), between schools and industry;
- use of the Internet and VLE to investigate and research school subjects, cross-curricular themes and topics related to social and personal development;
- use of the Internet and VLE to investigate careers and Further and Higher education;
- the development of pupils' competence in ICT skills and their general research skills.

b. On-line activities which are not permitted include, for example:

- searching, viewing and/or retrieving materials that are not related to the aims of the curriculum or future careers;
- copying, saving and/or redistributing copyright protected material, without approval;
- subscribing to any services or ordering any goods or services, unless specifically approved by the school;
- playing computer games or using other interactive 'chat' sites, unless specifically assigned by the teacher;
- using the network in such a way that use of the network by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages);
- publishing, sharing or distributing any personal information about a user (such as: home address; email address; phone number, etc.);
- sending or receiving unsavoury, insensitive, offensive or obscene e-mails
- any activity that violates a school rule.
- using any equipment to photograph, record or video any school activity for which explicit permission has not been given
- using or distributing any material relating to school activities, pupils or staff for which explicit permission has not been given
- engaging in any activity that is harmful of or hurtful to others

3. Sanctions

- a) Violation of the above rules will result in a temporary or permanent ban on Internet and VLE use.
- b) Additional disciplinary action may be added in line with existing school rules on inappropriate language or behaviour.
- c) Where applicable, police or local authorities may be involved.

4. Location and Supervision

- a) Internet and VLE access for pupils at Ballycastle High is located in the highly used ICT classrooms, the library and in most subject departments around the school. All such machines are in full view of people circulating in the area.



- b) While using the Internet and VLE at school, pupils **should, where possible**, be supervised directly by a member of staff. Independent electronic research requires specific teacher permission and research must be conducted in designated curricular areas only. In all cases, pupils should be reminded of their responsibility to use these resources in line with the school policy on acceptable use.
- c) Users will be made aware that the school has the ability to review files and communications to ensure that users are using the system responsibly. All uses of the Internet and VLE are logged and all sites visited by individual users are recorded. All e-mails can be read. While normal privacy is respected and protected by password controls, as with the Internet and VLE itself, **users must not expect Internet and VLE activity, e-mail or files stored on school servers to be absolutely private.**

5. Staff

- a) Teacher use of the C2K NI services by the Northern Ireland education community must be in support of the aims and objectives of the Northern Ireland Curriculum. C2K NI supports the implementation and sharing of effective practices and collaborative networking across the province, as well as nationally and internationally. Staff are encouraged to use C2K NI resources in their teaching and learning activities, to conduct research, and for contact with others in the education world.
- b) All school staff (both teachers and support staff) are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.
- c) cStaff are actively discouraged from communicating with pupils using social network sites or other technologies outside of school.

The Staff Acceptable Internet / Network Use Policy is published in the Staff Handbook and is attached as Appendix 2 at the end of this document.

6. Use of Digital Images of Pupils

All staff should follow the guidance below when dealing with taking, display storage and use of photographs and digital images of pupils.

Taking of Photographs/Video of Pupils

Staff should continue normal practice. Parents will be informed in writing and asked to give their consent to a range of such activities. Staff will be advised of those parents who withhold permission in due course.

Display/use of Photographs/Video of Pupils

Staff should continue normal practice for using photographs for display purposes in school. For displays/use outside school or where staff require additional guidance on the display/use of photographs the Principal or a member of the SMT **should be consulted.**



Storage of Photographs/Video of Pupils

It should **not be** normal practice to store digital images of pupils (however obtained) on school or personal laptops as a matter of course for **prolonged** periods of time.

As a result staff should ensure that:

1. Any image/s of a pupil/s (from camera, scanner or other source) that is/will be stored digitally should be stored on CD-ROM or external Hard Drive. Technical support will be available from the ICT department to assist in the transfer of existing/new images
2. After initial use by staff the images of pupils should be passed to the school ICT Co-ordinator for cataloguing and **centralised long-term storage**.
3. After initial use by staff digital images of pupils should be **deleted from laptops as soon as possible**.
4. Staff should not pass images of students via e-mail, CD-ROMs etc to third parties without consulting the Principal
5. Traditional photographs of pupils should continue to be stored within departments using scrapbooks or a suitable alternative.
6. If you require further advice consult the Principal or a member of the SMT. This guidance will be reviewed on an annual basis.

7. Information for Parents

Parents are informed **in writing** of the school policy on acceptable use of the Internet and VLE, and asked for permission for their children to use the Internet and VLE.

Students are also required to sign an undertaking agreeing to their proper use of the Internet and VLE. Details of the letter sent to parents and additional guidance information is included in the appendix to this policy. In addition to the above parents are given the following guidance by Ballycastle High School:

1. A home computer with Internet and VLE access should be situated in a location where parents can monitor access to Internet and VLE and e-mail. Computers should be fitted with suitable anti-virus, anti-spyware and filtering software.
2. Parents should agree with their children suitable days/times for accessing the Internet and VLE. Internet and VLE/e-mail usage can add significantly to your phone bill. Off-peak calls (after 6pm daily and weekends) are cheaper, but the cost of Internet and VLE access still needs to be carefully considered.
3. Parents should discuss with their children the school rules for using the Internet and VLE and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use;
4. Parents should get to know the sites their children visit, and talk to them about what they are learning;
5. Parents should consider using appropriate Internet and VLE filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below);
6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;



7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet and VLE, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images. If the message comes from an Internet and VLE service connection provided by the school or by C2K, they should immediately inform the school.

Further free advice for parents is available from the following sources:

<http://www.thinkuknow.co.uk/> - a website designed to inform children of the potential Hazards involved with online chatrooms.

<http://www.parentsonline.gov.uk/> - promotes home school links by helping parents understand the role of Information Communications Technology (ICT) in learning.

www.kidsmart.org.uk

<http://www.wiseuptothenet.co.uk/> - The Home Office guide to Internet safety with downloadable leaflets for parents

<http://www.getnetwise.org/> - information about filtering programs for home use

Protecting Your Home Computer

To protect a home computer, parents are advised to ensure the following items of software are installed on their home computers:

- Anti Virus Software: a free anti-virus software is available from AVG or Microsoft Security Essentials
- Anti Spyware Software: a free anti-virus software is included with Windows 7, Windows Vista and Windows XP (Service Pack 2 onwards). It is called Windows Defender.
- Filtering Software a free filtering software is provided by K-9 Bluecoat filtering software www.k9webprotection.com/

This policy acknowledges and complies with DENI circulars 1999/25 and 2007/01 on the subject of Acceptable Use of the Internet and VLE for Schools and DENI Circular 2011/22 on the subject of Internet Safety plus the Acceptable Use Policy developed by National Association of Co-ordinators and Teachers of IT

Appendix 1

Student Internet Permission Form

Dear Parent,

Internet Permission Form

You will, I am sure, already be aware that the Internet is the global network of computers which provides almost limitless access to unnumbered sources of information. As part of Ballycastle High School's ICT strategy we offer pupils supervised access to a *filtered* Internet service provided by C2k, the organization responsible for providing an ICT management service to every school in Northern Ireland. Before being allowed to use the Internet in School, all pupils need to obtain parental permission and both they and you should sign and return the enclosed form as evidence of your approval and their acceptance of the school policy and rules which govern their access.

Access to the Internet will enable pupils to explore thousands of libraries, databases, and bulletin boards while exchanging messages with other Internet users throughout the world. Whilst our aim for Internet use is to further educational goals and objectives, families should be warned that there is, of course, material potentially available, which may contain illegal, defamatory, inaccurate or offensive items.

We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, far exceed any potential disadvantages. We have, therefore, put in place a filtered Internet and e-mail service to minimize the dangers of pupils gaining access to unsuitable material. In addition a clear set of rules and procedures for pupil use has been implemented. Ultimately, however, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will guide pupils towards appropriate and relevant materials. Clear rules and procedures are in place for proper use. Outside of school, families bear the same responsibility for such guidance as they exercise with other information sources such as television, telephones, films, radio and other also potentially offensive media. Home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and school work. It should, however, be supervised, and parents should be aware that they are responsible for their children's use of Internet resources at home.



In addition to the enclosed guidance documents free advice for parents is available from the following sources:

<http://www.thinkuknow.co.uk/> - a website designed to inform children of the potential hazards involved with online chatrooms.

<http://www.parentsonline.gov.uk/> - promotes home school links by helping parents understand the role of Information Communications Technology (ICT) in learning.

www.kidsmart.org.uk

<http://www.wiseuptothenet.co.uk/> - The Home Office guide to Internet safety with downloadable leaflets for parents

<http://www.getnetwise.org/> - information about filtering programs for home use

We would be grateful if you could read the enclosed guidance documents and then complete the permission form which follows.

Yours sincerely
I Williamson
Principal



Please complete and return this form to school.

Internet Parent Permission Form

Name of Pupil: _____

Date of Birth: _____

Pupil

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Pupil Signature: _____ Date: _____

Parent

As the parent or legal guardian of the pupil signing above, I grant permission for my son to use electronic mail and the Internet. I understand that pupils will be held accountable for any use of the Internet in School or outside School when it is deemed to have an impact on the School or its pupils. I also understand that some materials on the Internet may be inappropriate and offensive and I accept responsibility for setting standards outside School for my son to follow when selecting, sharing and exploring computer information and media.

Parent Signature: _____ Date: _____



Additional Advice for Parents with Internet access at Home

1. The computer with Internet access should be situated in a location where parents can monitor access to Internet. Computers should be fitted with suitable anti-virus, anti-spyware and filtering software.
2. Parents should agree with their children suitable days/times for accessing the Internet. If using dial-up accounts, Internet usage can add significantly to your phone bill. Off-peak calls (after 6pm daily and weekends) are cheaper, but the cost of Internet access still needs to be carefully considered. Fixed-price broadband services represent the best value for money.
3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long, and what comprises appropriate use;
4. Parents should get to know the sites their children visit, and talk to them about what they are learning;
5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available below.
6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;
7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school or by C2k, they should immediately inform the school.



Further free advice for parents is available from the following sources:

<http://www.thinkuknow.co.uk/> - a website designed to inform children of the potential hazards involved with online chatrooms.

<http://www.parentsonline.gov.uk/> - promotes home school links by helping parents understand the role of Information Communications Technology (ICT) in learning.

www.kidsmart.org.uk

<http://www.wiseuptothenet.co.uk/> - The Home Office guide to Internet safety with downloadable leaflets for parents

<http://www.getnetwise.org/> - information about filtering programs for home use

Protecting Your Home Computer

To protect your home computer, parents are advised to ensure the following items of software are installed on their home computers:

- Anti Virus Software: free anti-virus software is available from AVG
- Anti Spyware Software: free anti-virus software is included with Windows Vista and Windows XP (Service pack 2 onwards). It is called Windows Defender.
- Filtering Software free filtering software is provided by K-9 Bluecoat filtering software www.k9webprotection.com/

