DUNDONALD
HIGH SCHOOL

ACCEPTABLE USE OF THE INTERNET, VLE AND DIGITAL IMAGES

Policy

Policy Details

Last Review Date	New Version Date	Date Ratified by BOG	Next Review	Responsible
October 2016	November 2018	November 2018	November 2021	M. Perry

Dundonald High School Policy for the Acceptable Use of the Internet and VLE

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

Dundonald 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, Dundonald High School has invested in providing networked Internet and VLE Access to pupils free of charge at stations on the school network, 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 and VLE and e-mail during KS3 ICT classes. Appropriate cross-curricular use of the Internet and VLE is encouraged. Staff at Dundonald High School are currently undergoing training in the use of the Internet and VLE within the curriculum. The Internet and VLE can also play a key role in supporting the Careers and LLW departments.

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

• In ICT lessons
• Through subject use across the curriculum
• In the ICT club
• During normal school hours and lunch-times for specified research purposes with the permission of a teacher

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 Dundonald High School.

Promoting Awareness with Parent, Governor and Community

Dundonald 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

In addition, regular references will be made to the policy in communications with stakeholders. Occasionally, Dundonald High School may hold information events/special events to promote greater awareness of interest in the policy.

DUNDONALD HIGH SCHOOL POLICY FOR THE ACCEPTABLE USE OF THE INTERNET AND VLE

1. For Staff and 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.

b) Dundonald High School 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) Staff and students at Dundonald High School 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) Dundonald 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 Dundonald 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 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 inappropriate, insensitive, offensive or obscene images or e-mails
• any activity that violates a school rule.

c. Other activities which are not permitted include-

- 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 Dundonald High School is located in the highly used ICT classrooms, the library and in some 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 **must** be supervised directly by a member of staff or indirectly by a technician or librarian. 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 Use of Internet and VLE

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. Staff may request training in use of Internet and VLE and e-mail at any time.

b. The Internet and VLE and e-mail training for staff will also focus on how electronic information-handling skills are now considered fundamental to the preparation of citizens and future employees in the Information Age. Staff will be encouraged to investigate the possibilities provided by access to this electronic information and communication resource, and blend its use, as appropriate, within the curriculum. Staff will be encouraged to identify appropriate and effective use of such skills, and provide guidance and instruction to pupils in the acceptable use of the Internet and VLE.

c. 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.

d. All staff are expected to have undertaken appropriate Health and Safety Training in the correct use of ICT equipment.

e. All staff have undertaken appropriate GDPR Training in the correct use of ICT equipment and storing and sharing personal data.

f. Staff are actively discouraged from communicating with pupils using social network sites or other technologies outside of school.

6. Acceptable 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 in line with GDPR guidance also.

Taking of Photographs/Video of Pupils

Staff should continue normal practice. Parents will be informed in writing or verbally 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 the C2K system. Technical support will be available from the ICT Technician to assist in the transfer of existing/new images to the system.
2. After initial use by staff digital images of pupils should be deleted from laptops as soon as possible.
3. Staff should not pass images of students via e-mail etc to third parties without consulting the Principal
4. Traditional photographs of pupils should continue to be stored within departments using scrapbooks or a suitable alternative.

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 to permission for their child/children to use the Internet and VLE. Students are also required to sign an agreement 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 Dundonald 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 inappropriate 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

DUNDONALD HIGH SCHOOL
Staff Acceptable Internet / Network Use Policy
Reviewed June 2018

Computer and network access, including internet access, is designed to provide staff with a valuable educational resource for the benefit of the pupils and to support the delivery of the curriculum. It should also enhance teaching, research, preparation, provision of classroom materials, administration and management, as well as facilitate the sharing of resources, communications and co-operation within and between departments. Members of staff are responsible for their own communications and their use of the network.

This policy is designed primarily to help and protect staff in their use of network material and to clarify what the school considers to be acceptable practice.
Staff should be aware that files stored on school servers and computers [including laptops] will not be regarded as private. The school reserves the right to monitor, review and examine the internet history, usage, communications and files of all users, and, where it deems it to be necessary, will intercept and delete material on school laptops, servers, network devices and e-mail systems, which it considers inappropriate, and prohibit the use of such material.

The school expects and requires all users to comply with the standards outlined in this policy and to follow its protocols.

Use of the network will imply acceptance of this policy.

General Protocols

• All uses of the system, including all internet activity, which occurs during the school day, between 8.30 am and 4.30 pm, must be relevant to the delivery of the curriculum and to the general life of the school. Users should, at all times, exercise extreme caution in the type of material downloaded and viewed.

• Access to the network should only be made via the user's authorised account and Password, which should**, in no circumstances**, be made available to any other person inside or outside the school. The school's C2K managers will have access to all users accounts on the network.

• Users are responsible for all e-mails sent and for any contacts which may result in e-mails being received.

• Standards of expression and conduct, which apply in hard copy communications from the school, should also apply in all electronic communications. No material which would reflect badly upon the school's reputation, including defamatory messages, indecent material, pornography, offensive language or images, should be sent from the school's system.

• All laws, including those of copyright, should be respected in internet and network use. Copyrighted or unlicensed software should not be unlawfully duplicated.

• Only software approved by the school's C2K managers may be used on the school's system and equipment, including laptops. Prior approval must always be sought. Unauthorised software installation, which may cause a laptop or computer to fail, will incur a charge from Sx3 for repair.

• Activity which threatens the integrity or security of the school system, such as the unauthorised installation of software or hardware, or which compromises other systems, is forbidden.
• The use of the internet to access inappropriate material (e.g. pornographic, racist or otherwise offensive material) is forbidden.

Data Security
• All staff share the school's responsibility under data protection legislation and GDPR.
All staff have received GDPR training regarding current legislation in November 2018.
• Information about the school, and its pupils, must be closely safeguarded. Care should be taken to ensure that information held on school systems, including laptops, is not lost, disclosed, modified without authorisation or accessed by third parties.
• Computers, including laptops, must never be left unattended in an open classroom or other insecure location.
• Users of the school network are responsible for the security of their computers / laptops and should NEVER leave the computer unattended when logged on to the network.
Security of data requires that the user locks, logs off or shuts down the station **every time** the computer is unattended. The SIMS Launcher, in particular, must be closed down every time a station is left unattended. At the end of the working day, each station must be shut down to enable the backup of files to proceed.

Security of Equipment
• It is important that staff exercise due care to ensure that school IT equipment is protected from damage or theft.
• Laptops should be kept in a locked cupboard or locked room overnight or when not in use for long periods of time. Laptops must never be left unattended in a car and must be kept out of the reach of children.
• Theft or loss of school equipment must be reported immediately to a C2K manager.

Access to data/information
• If files, belonging to another member of staff, are inadvertently accessed, it must be reported immediately to a C2K manager, so that corrective action may be taken to protect the accessed files.

Viruses
• All staff should be aware of the potential damage that a virus can do to the school's IT infrastructure. Extreme caution should be exercised when importing files on to the school's network from another system. Any staff member, who becomes aware of a virus outbreak, should immediately contact a C2K manager.
• C2K updates the virus software daily. In the interests of the integrity of the network,
Laptops must be connected to the network in school **once a week** to ensure updates are downloaded.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook or MySpace or when gaming on the internet, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave users open to abuse, and often make little or no distinction between adult users and children.

Staff should not allow any pupil to access personal information you post on a social networking site. In particular:

- Staff **should not** add a pupil to their 'friends list'.
- Staff **should not** communicate with or play with a pupil when gaming on the internet.
- Staff **should** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- Staff should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
- Staff should take steps to ensure that any person contacting them via a social networking website is who they claim to be, and not an imposter, before allowing them access to their personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, staff **must not** post content on websites that may appear as if you are speaking for the school.
- Staff should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- Staff should avoid posting any material clearly identifying themself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Use of E-mail

All members of staff with a computer account are provided with an e-mail address for communication both internally and with other e-mail users outside the school. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. Staff **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. Staff **must not**

purchase goods or services on behalf of the school via e-mail without proper authorisation.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, staff **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school, in conjunction with C2K, will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- Staff must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Pupil Use

- Pupils **must** be supervised at **all** times when using school computer equipment. When arranging use of computer facilities for pupils, staff must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the C2K does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
- Staff should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).
- The school may also use measures to audit use of computer systems for performance and diagnostic purposes.
- **Use of the school computer system indicates your consent to the above described monitoring taking place.**

Confidentiality and Copyright

- Staff must respect the work and ownership rights of people outside the school, as well as other staff or pupils.
- Staff are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), they should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

- Staff **must** consult a C2K Manager before placing any order of computer hardware or software, or obtaining and using any software they believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by a member of staff during the course of their employment in any way affecting or relating to the business of the School or capable of being used or adapted for use within the School shall be immediately disclosed to the School and shall to the extent permitted by law belong to and be the absolute property of the School.

By storing or creating any personal documents or files on the school computer system, staff grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

Reporting Problems with the Computer System

It is the job of the C2K Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- Staff should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder their job or teaching and require immediate attention should be reported by telephone or e-mail.
- If a member of staff has lost documents or files, they should report this as soon as possible.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. Staff **must** immediately inform the C2K Manager, or the Principal, of abuse of any part of the computer system. In particular, they should report:

- any websites accessible from within school that they feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in e-mail, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by them, another member of staff, or a pupil via the school computer system.

Reports should be made either in person or via email. All reports will be treated confidentially.

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 the Acceptable Use Policy developed by National Association of Co-ordinators and Teachers of IT

Dear Parent/Guardian,

INTERNET PERMISSION LETTER

The Internet is the global network of computers you will have read about and seen on television. As part of the Dundonald High School's ICT strategy we offer pupils supervised access to a *filtered* Internet service provided by c2k. Before being allowed to use the Internet, all pupils must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules on this matter.

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. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. We have put in place a filtered Internet and e-mail service to minimise the dangers of pupils gaining access to unsuitable materials. In addition a clear set of rules and procedures for pupil use of the Internet has been implemented. But ultimately, 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 will toward appropriate materials. Clear rules and procedures are in place for proper use of the Internet. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media. Appropriate 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

M K Perry
PRINCIPAL

Please complete and return this form to the school.

Internet Parent Permission Form

Name of Pupil: _____

Form class: _____

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 or daughter to use electronic mail and the Internet. I understand that pupils will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or 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 inappropriate 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

DUNDONALD HIGH SCHOOL
Staff Acceptable Internet / Network Use Policy

Computer and network access, including internet access, is designed to provide staff with a valuable educational resource for the benefit of the pupils and to support the delivery of the curriculum. It should also enhance teaching, research, preparation, provision of classroom materials, administration and management, as well as facilitate the sharing of resources, communications and co-operation within and between departments. Members of staff are responsible for their own communications and their use of the network.

This policy is designed primarily to help and protect staff in their use of network material and to clarify what the school considers to be acceptable practice.
Staff should be aware that files stored on school servers and computers [including laptops] will not be regarded as private. The school reserves the right to monitor, review and examine the internet history, usage, communications and files of all users, and, where it deems it to be necessary, will intercept and delete material on school laptops, servers, network devices and e-mail systems, which it considers inappropriate, and prohibit the use of such material.

The school expects and requires all users to comply with the standards outlined in this policy and to follow its protocols.

Use of the network will imply acceptance of this policy.

General Protocols

• All uses of the system, including all internet activity, which occurs during the school day, between 8.30 am and 4.30 pm, must be relevant to the delivery of the curriculum and to the general life of the school. Users should, at all times, exercise extreme caution in the type of material downloaded and viewed.

• Access to the network should only be made via the user's authorised account and Password, which should**, in no circumstances**, be made available to any other person inside or outside the school. The school's C2K managers will have access to all users accounts on the network.

• Users are responsible for all e-mails sent and for any contacts which may result in e-mails being received.

• Standards of expression and conduct, which apply in hard copy communications from the school, should also apply in all electronic communications. No material which would reflect badly upon the school's reputation, including defamatory messages, indecent material, pornography, offensive language or images, should be sent from the school's system.

• All laws, including those of copyright, should be respected in internet and network use. Copyrighted or unlicensed software should not be unlawfully duplicated.

• Only software approved by the school's C2K managers may be used on the school's system and equipment, including laptops. Prior approval must always be sought. Unauthorised software installation, which may cause a laptop or computer to fail, will incur a charge from Sx3 for repair.

• Activity which threatens the integrity or security of the school system, such as the unauthorised installation of software or hardware, or which compromises other systems, is forbidden.
• The use of the internet to access inappropriate material (e.g. pornographic, racist or otherwise offensive material) is forbidden.

Data Security
• All staff share the school's responsibility under data protection legislation in line with GDPR legislation May 2018.
• Information about the school, and its pupils, must be closely safeguarded. Care should be taken to ensure that information held on school systems, including laptops, is not lost, disclosed, modified without authorisation or accessed by third parties.
• Computers, including laptops, must never be left unattended in an open classroom or other insecure location.
• Users of the school network are responsible for the security of their computers / laptops and should NEVER leave the computer unattended when logged on to the network.
Security of data requires that the user locks, logs off or shuts down the station **every time** the computer is unattended. The SIMS Launcher, in particular, must be closed down every time a station is left unattended. **At the end of the working day, each station must be shut down to enable the backup of files to proceed.**

Security of Equipment
• It is important that staff exercise due care to ensure that school IT equipment is protected from damage or theft.
• Laptops should be kept in a locked cupboard or locked room overnight or when not in use for long periods of time. Laptops must never be left unattended in a car and must be kept out of the reach of children.
• Theft or loss of school equipment must be reported immediately to a C2K manager.

Access to data/information
• If files, belonging to another member of staff, are inadvertently accessed, it must be reported immediately to a C2K manager, so that corrective action may be taken to protect the accessed files.

Viruses
• All staff should be aware of the potential damage that a virus can do to the school's IT infrastructure. Extreme caution should be exercised when importing files on to the school's network from another system. Any staff member, who becomes aware of a virus outbreak, should immediately contact a C2K manager.
• C2K updates the virus software daily. In the interests of the integrity of the network,
Laptops must be connected to the network in school **once a week** to ensure updates are downloaded.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites such as Facebook or MySpace or when gaming on the internet, even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave users open to abuse, and often make little or no distinction between adult users and children.

Staff should not allow any pupil to access personal information you post on a social networking site. In particular:

- Staff **should not** add a pupil to their 'friends list'.
- Staff **should not** communicate with or play with a pupil when gaming on the internet.
- Staff **should** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
- Staff should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
- Staff should take steps to ensure that any person contacting them via a social networking website is who they claim to be, and not an imposter, before allowing them access to their personal information.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, staff **must not** post content on websites that may appear as if you are speaking for the school.
- Staff should not post any material online that can be clearly linked to the school that may damage the school's reputation.
- Staff should avoid posting any material clearly identifying themself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

Use of E-mail

All members of staff with a computer account are provided with an e-mail address for communication both internally and with other e-mail users outside the school. The following considerations must be made when communicating by email:

- E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. Staff **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail.
- E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. Staff **must not**

purchase goods or services on behalf of the school via e-mail without proper authorisation.
- E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, staff **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, or other confidential information belonging to the school.
- Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school, in conjunction with C2K, will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
- Staff must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

Supervision of Pupil Use

- Pupils **must** be supervised at **all** times when using school computer equipment. When arranging use of computer facilities for pupils, staff must ensure supervision is available.
- Supervising staff are responsible for ensuring that the separate Acceptable Use Policy for pupils is enforced.
- Supervising staff **must** ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by pupils.

Privacy

- Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the C2K does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
- Staff should avoid storing sensitive personal information on the school computer system that is unrelated to school activities (such as personal passwords, photographs, or financial information).
- The school may also use measures to audit use of computer systems for performance and diagnostic purposes.
- **Use of the school computer system indicates your consent to the above described monitoring taking place.**

Confidentiality and Copyright

- Staff must respect the work and ownership rights of people outside the school, as well as other staff or pupils.
- Staff are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), they should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.

- Staff **must** consult a C2K Manager before placing any order of computer hardware or software, or obtaining and using any software they believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.
- As per the standard staff contract, any invention, improvement, design, process, information, copyright work, trade mark or trade name made, created or discovered by a member of staff during the course of their employment in any way affecting or relating to the business of the School or capable of being used or adapted for use within the School shall be immediately disclosed to the School and shall to the extent permitted by law belong to and be the absolute property of the School.

By storing or creating any personal documents or files on the school computer system, staff grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

Reporting Problems with the Computer System

It is the job of the C2K Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

- Staff should report any problems that need attention to a member of IT support staff as soon as is feasible. Problems that seriously hinder their job or teaching and require immediate attention should be reported by telephone or e-mail.
- If a member of staff has lost documents or files, they should report this as soon as possible..

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. Staff **must** immediately inform the C2K Manager, or the Principal, of abuse of any part of the computer system. In particular, they should report:

- any websites accessible from within school that they feel are unsuitable for staff or student consumption;
- any inappropriate content suspected to be stored on the computer system. This may be contained in e-mail, documents, pictures, etc;
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by them, another member of staff, or a pupil via the school computer system.

Reports should be made either in person or via email. All reports will be treated confidentially.