Down High School

Whole School

E-Safety Policy

Adopted 3/2/15

(Abridged Version)

Down High School Whole School E-Safety Policy

Updated September 2017

Introduction

Information and Communication Technology (ICT), comprising the Internet and any other form of digital information and communications technology, has become integral to the lives of children and young people both within educational establishments and in their lives outside school. ICT provides powerful tools which open up new learning opportunities for everyone. ICT can stimulate discussion, promote creativity and contribute to effective learning. Students, staff and the wider community have an entitlement to safe use of ICT at all times. This e-safety policy sets out a framework to ensure safe and appropriate use of ICT at Down High School.

E-Safety Education at Down High School

E-Safety education focuses on the safe use of ICT tools and technologies. E-Safety education is designed to make users aware of the measures they can take to:

- safeguard ICT tools and technologies from virus, malware and other attacks;
- safeguard themselves when using ICT tools and technologies;
- safeguard others when using ICT tools and technologies.

The purpose of E-Safety Education at Down High School is to:

- ensure users make **safe and informed choices** about their use of ICT tools and technologies;
- educate users to enable users to **protect themselves from harm;**
- educate users to enable users to protect **the ICT tools and technologies they use from harm;**
- ensure users know **how to seek help** and **how to report concerns** about any e-safety issue.

How is E-Safety Education Delivered at Down High School?

- E-Safety education is taught as part of KS3 ICT curriculum, delivered to staff as part of CPD and communicated to parents as part of this whole-school e-safety policy.

- E-Safety education is supported by the following policies adopted by Down High School:

  - Whole School E-Safety Policy.
  - Acceptable Use of ICT Policy for Students and Staff.
  - Bring Your Own Device Policy.
  - Guidelines on Safe Use of Educational Video in the Classroom.
  - ICT Health and Safety Policy.

Rationale for student use of the ICT

Down High School encourages use by learners of the rich information sources available using ICT, together with the development of appropriate skills to analyse and evaluate such resources. On-line resources offer a broad 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, VLE and e-mail literacy are fundamental requirements for all learners as preparation for the Information Age – an era where ICT is a dominant factor in work and home life.

Access Arrangements School ICT Facilities

In recognition of these benefits Down High School, in conjunction with C2K, has invested in providing networked internet access to learners free of charge at C2K 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 and staff will be provided with appropriate training and guidance on how to use the Internet, school VLE and e-mail safely during KS3 ICT classes. Appropriate cross-curricular use of the ICT facilities is encouraged.

How will pupils gain access to ICT at Down High School?

- In ICT lessons;
- through subject use across the curriculum;
- in after-school clubs;
- in the Sixth Form, using either C2K or BYOD devices, during normal school hours; and lunch-times for specified research purposes with the permission of a teacher.

Are there any dangers in using ICT?

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student motivation and achievement. However, the use of these new technologies can put students and staff at risk within and outside the school. The internet is vast and unregulated and, in common with all communication media, there remains the concern that it can be abused. Since it 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.

Some of the dangers users may face include:

- exposure to unacceptable materials (pornographic, violent, extremist literature);
- encountering inappropriate messages (harassing, demanding, belligerent contacts);
- arranging contacts and meetings (potential exploitation, grooming and physical dangers);
- inadvertently provide personal information whilst on-line which could be sufficient to put them in danger or to allow commercial companies to exploit them;
- unauthorised access to, loss of or sharing of personal information;
- the sharing/distribution of personal images without an individual's consent or knowledge;
- cyber-bullying;
- access to unsuitable video/Internet games;
- an inability to evaluate the quality, accuracy and relevance of information on the Internet;
- plagiarism and copyright infringement;
- illegal downloading of music or video files;
- the potential for excessive use which may impact on the social and emotional development and learning of the young person;
- injury through not observing correct Health and Safety guidelines in relation to ICT.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Positive Behaviour and Child Protection. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school. The school may inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through a planned programme of e-safety education, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

E-Safety –Student Education at Down High School

E-safety education will be provided in the following ways:

- a planned e-safety programme is delivered as part of the taught ICT curriculum at KS3. This programme covers the safe use of ICT facilities, the Internet, VLE and digital technologies both in school and outside of school and how to identify and deal with cyber-bullying;
- students are taught safe working practices and are required to follow all Health and Safety guidelines;
- students are taught in lessons to use ICT safely and how to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information;
- students are helped to understand the need for the Student Acceptable Use Policy (AUP) and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school;
- students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- rules for the proper and safe use of ICT systems and the Internet are posted in school;
- staff act as good role models in their use of ICT, the Internet and mobile devices.

If a student has any concerns regarding e-safety they should report these directly to their form teacher.

E-Safety - Staff Education at Down High School

- Down High School will provide training and support to staff in e-safety issues, including making all staff aware of safe use of ICT equipment and the procedures that need to be followed in the event of an e-safety incident taking place;
- all new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety AUP and Child Protection Policies;
- staff will receive regular updates through DENI, C2K, SEELB and/or other information/training sessions/guidance documents;
- **governors** are invited to take part in e-safety training and awareness sessions.

If a member of staff has any concerns regarding e-safety they should report these directly to the whole school ICT leader or a member of the SMT.

E-Safety – Information and Support for Parents/Carers

- Down High School will provide annual guidance/information to and, where appropriate, arrange briefings for parents/carers on a range of e-safety issues.

If a parent has any concerns regarding e-safety they should report these directly to their son's/daughter's form teacher. In the case of a serious incident the PSNI should be contacted for advice.

E-Safety - Acceptable Use Policy

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 student to educate the student about his or her responsibility when using ICT. The following sets out the policy for acceptable use of the ICT at Down High School.

- **Students** will be required to read through and sign the E-Safety Acceptable Use Policy (AUP) to ensure they understand the rules relating to safe and acceptable use of ICT.

- **Parents/carers** will be required to read through and sign the E-Safety AUP alongside their child's signature, helping to ensure their children understand the rules before the necessary permissions are given for children to access the full range of ICT resources while at school.

- **Staff and regular visitors** to the school have a Staff E-Safety AUP that they must read through and sign to indicate understanding of the rules.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this E-Safety Policy is followed. Students and staff **must** immediately inform the whole school ICT leader 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;
- any instance of bullying or harassment suffered by them, another member of staff, or a student via the school computer system.

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

Roles and Responsibilities

Roles and responsibilities relating to this policy are outline in Appendix 1.

Scope

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school.

Acknowledgements

This policy acknowledges and complies with DENI circulars 2013/25, 2007/01 and 1999/25 on the subject of Acceptable Use of the Internet and VLE for schools; the
Acceptable Use Policy developed by the National Association of Co-ordinators and Teachers of IT; the e-safety policy developed by Netherwood School UK and the resources provided on e-safety by Kent LEA.

Appendix 2: Down High E-Safety Acceptable Use of ICT Policy

1. For Pupils

a) Pupils are responsible for good behaviour and safe working practices when using ICT just as they are in the classroom or a school corridor. General school rules apply. In addition, a number of rules relating to the safe use of the ICT also apply.

b) Down High School has implemented a filtered Internet service through C2K, a filtered e-mail service (as recommended by UK government) through C2K and its own VLE which can be accessed via the school website. Pupils are **not permitted** to use any other internet or e-mail service in school.

Internet and e-mail services are monitored and are not therefore private – internet activity and email messages can be viewed at any time.

c) Pupils at Down High School should **know and understand** that no ICT 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;
- gain access to another user's account;
- 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 (e.g. buying or selling items on eBay) or to access social networking sites;
- use ICT resources in any way that contravenes the ICT Health and Safety policy.

Pupils must not post on the internet (or transmit via any mobile communication device) any comments or images or engage in any online behaviours which might cause harm or offence to fellow pupils, staff or other members of the school community.

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

e) Down High School will make every reasonable effort to ensure that all pupils understand how they are to use the ICT appropriately and why the rules exist. Pupils will be directed to the student version of this policy on first using ICT, and during subsequent sessions as changes are made/issues arise.

f) ICT facilities are 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 ICT 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, mobile communication devices, movies, radio, and other potentially offensive media.

h) When using ICT facilities at Down High School, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws.

i) When using ICT facilities at Down High School, all users must comply with all Health and Safety guidelines.

2. Examples of Acceptable and Unacceptable Use

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

- the appropriate use of email and computer conferencing for communication between colleagues, between student(s) and teacher(s), between student(s) and student(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 ICT 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, accessing any social networking sites 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);
- using any software other than that provided by the c2k system;
- 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;
- 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;
- any activity that violates a school rule;
- engaging in any activity that is harmful or hurtful to others;
- not following the correct Health and Safety guidelines relating to the safe use of ICT.

c. Cyber Bullying

Through education and training, pupils and staff will be made aware of cyber bullying risks and are expected to be vigilant both in and out of school and report any concerns to a trusted adult. Cyber bullying is a form of bullying and will be dealt with through the whole-school anti-bullying policy, positive behaviour policy and through the pastoral care system.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or abusive emails which may include viruses or inappropriate content.
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity.
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile.
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites.
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people.
- Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

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

- Protection from Harassment (NI) Order 1997.
- Malicious Communications (NI) Order 1988.
- The Communications Act 2003.

Reporting Incidents of Cyber Bullying

Pupils are encouraged to report incidents of cyber-bullying to both their form teacher and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases.

Down High School will keep appropriate pastoral care records of cyber-bullying incidents to monitor the effectiveness of their preventative activities, and to review and ensure consistency in their investigations, support and sanctions.

Access to social media (e.g. Facebook, Twitter etc) in school is prohibited.

Securus

'Securus' is an e-Safety monitoring system purchased and provided by C2K that helps teachers identify cyber-bullying and other child protection concerns. On detection of inappropriate words or phrases, an alert is sent to nominated individuals (pastoral staff) to allow immediate intervention and action.

Down High School will use the Securus system as implemented by C2K.

3. Sanctions

a) Violation of the above rules will result in a temporary or permanent ban on using key parts of ICT facilities e.g. Internet, VLE etc.
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) ICT access for pupils at Down 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 ICT 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, it is the pupils' 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 ICT facilities 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 themselves, **users must not expect ICT, internet and VLE activity, e-mail or files stored on school servers to be absolutely private**.

5. Staff Use of ICT Facilities

a. Teacher use of the C2K services must be in support of the aims and objectives of the Northern Ireland Curriculum. C2K 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 resources in their teaching and learning activities, to conduct research, and for contact with others in the education world. Staff may request training in e-safety, use of Internet and e-mail at any time.

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. Staff are actively discouraged from communicating with pupils using social networking sites, mobile communication devices or other technologies outside of school. Email communication between staff and pupils should only be by means of C2k email addresses - for both staff and pupils. The Staff Acceptable Use of the ICT, Internet, Network and VLE Policy is published in the Staff Handbook and is attached as Appendix 2.

6. Incident Monitoring and Reporting

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the appropriate member(s) of staff depending on the severity of the incident.

- The C2K service will record any breaches, suspected or actual, of the filtering systems
- The incident should be investigated by the Whole School ICT leader and reported to an appropriate member of the SMT.

7. Information for Parents

Parents are informed **in writing** of the school policy on acceptable use of the ICT and asked for permission for their child/children to use these ICT. Students are also required to sign an undertaking agreeing to their proper use of ICT. 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 further guidance by Down High School (Appendix 1) and invited to e-safety briefings.

If a parent is concerned about any instance of e-safety they should report this concern directly to their son/daughter's form teacher.

Appendix 3: Student E-Safety ICT Permission Form

Dear Parent,

E-Safety ICT Permission Form

You will, I am sure, already be aware that safe use of ICT is a key part of a student’s modern learning experience. As part of Down High’s ICT strategy we offer pupils supervised access to a filtered Internet service and a filtered e-mail service, both provided by C2K, the organization responsible for providing an ICT management service to every school in Northern Ireland. The school also provides access to a VLE via the Down High website. Before being allowed to use the Internet, VLE and email, 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 e-safety policy and rules and responsibilities 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 aims 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 potentially offensive items.

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, therefore, 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 student use of the Internet 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 toward appropriate 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 information sources such as television, telephones, mobile communication devices, movies, radio and other 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. I would also stress the importance of your son/daughter following appropriate ICT Health and Safety guidelines to ensure safe working practices at home.

I would wish to emphasise that the school’s acceptable use policy prohibits pupils from harassing, insulting or attacking any member of the school community through the use of ICT. The incidence of cyber bullying has risen in recent years. I would encourage all parents to check regularly with their son/daughter that they are neither a victim of nor are they engaging in any behaviour that could be considered cyber bullying. Cyber bullying incidents should be reported directly to the school. It may also be necessary to report serious incidents of cyber bullying directly to the PSNI.

If you have any concerns regarding e-safety you should report these directly to your son’s/daughter’s form teacher.

In addition to the attached guidance notes, free advice for parents is available from the following sources:

- **http://www.downhighschool.org.uk** - Down High School E-Safety policy – see Information For Parents section of the Down High School web site.

• http://www.thinkuknow.co.uk a website designed to inform children and parents about potential online hazards and promote internet safety for children, run by the Child Exploitation and Online Protection Centre

• http://www.kidsmart.org.uk a website designed to inform children and parents about potential online hazards and promote internet safety for children.

• http://www.getnetwise.org/ - information about e-safety and filtering programs for home use

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

Yours sincerely

Mrs M Perry

Principal

Down High School E-Safety Permission Form

Please complete and return this form to the main school office.

Name of Student: ________________________________Form class: ____________

Student
As a school user of ICT, I agree to comply with the school rules on its use.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any software that might allow me to bypass the filtering and security systems in place.
- I will not try to install software on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/iPod) in school at times that are permitted.
- When using my own devices, I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet ‘on-line friends’ unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I understand that chat and social networking sites are not permitted.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.
- I will not threaten, harass, cyber bully or otherwise cause harm or distress to other members of the school or wider community
- I will use the network in a responsible way and observe all the restrictions explained to me by the school.
- I understand that the school and C2K may monitor my email and Internet activity and that files on the school network are not totally private.

- I agree to be responsible and stay safe while using ICT.

- I understand that irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.
- I will follow all ICT Health and Safety guidelines.

Student Signature: ________________________ **Date:** ______________

Parent

As the parent or legal guardian of the student signing above, I grant permission for my son or daughter to use ICT. I understand that pupils will be held accountable for any use of the ICT in school or outside school when it is deemed to have an impact on the school or its pupils. **I understand that the school and C2K may monitor the e-mail, VLE and Internet activity of my son/daughter and that files stored on the school network are not totally private.** 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.

I understand that if I have any objections to my son / daughter featuring in school photographs, videos or other promotional materials that I must register these in writing to the Principal.

Parent Signature: ________________________ **Date:** _________________

Key Definitions

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 users. The educational value of appropriate use of information and resources located on the Internet 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. The Down High School VLE will be accessible via the school website.

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, antispyware and filtering software.

2. Parents should agree with their children suitable days/times for accessing the Internet. Internet/e-mail usage can add significantly to your phone bill. 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 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 filtering software for blocking access to unsavoury materials.

6. Parents should be aware of the potential risks of giving children unmonitored access to newsgroups, chat facilities or social networking sites.

7. Pupils should not post on the Internet (or transmit via mobile communication devices) any comments or images which might cause harm or offence to fellow pupils or staff.

8. 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.

9. 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.

10. The C2K Internet and e-mail service is monitored. As such all visits to internet sites are logged and all e-mails can be read.

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

http://www.downhighschool.org.uk - School E-Safety policy – see Information For Parents section of the site.

- http://www.thinkuknow.co.uk a website designed to inform children and parents about potential online hazards and promote internet safety for children, run by the Child Exploitation and Online Protection Centre

- http://www.kidsmart.org.uk a website designed to inform children and parents about potential online hazards and promote internet safety for children.

- http://www.getnetwise.org/ - information about e-safety and 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: free anti-virus software is available from a number of companies including AVG (www.avg.com), Avast! (www.avast.com) and Avira (www.free-av.com). Subscription services are also available from Norton (www.norton.com), McAfee (www.mcafeestore.com) and a number of other companies.
- 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. Ant-virus software may also be obtained from the websites indicated above and from other sources.
- Filtering Software: internet filter and parental control software is available at www.k9webprotection.com. Other products available on the market include Net Nanny, McAfee Family Protection and CYBERsitter.

Health and Safety Guidelines - Safe Use of a Home Computer

All ICT equipment and the electrical supply to which it is connected should be checked regularly for defects.

Parents should encourage their children to adopt sensible postures when using ICT equipment (feet flat on ground; back firmly supported by an adjustable, swivel chair).

Heating, lighting and ventilation should be considered carefully to reduce excess heat; screen glare. Adequate air flow needs to be maintained in rooms where printers are used.

Monitors where used should be able to both tilt and swivel. Keyboards should be height adjustable. Keyboard and foot rests should be provided as needed. Headphones/speakers should be adjusted to normal sound levels at all times. Permanent ear damage can result from sound level set too high.

E-SAFETY ADDITIONAL INFORMATION

Websites

Down High School Website

The Down High School website is intended to:

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

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 acceptable.

The point of contact on the web site will be the school address, telephone number and email address. Home information or individual e-mail identities will not be published.

School website address: www.downhighschool.org.uk

Social Networking Sites

Students are not permitted to use social networking sites at school.

Parents should be aware that it is **illegal for children under the age of 13** to be registered on/using certain social networking sites.

Students in the KS3 curriculum will be taught about e-safety on social networking sites to encourage responsible use outside of school.

Passwords

- A password policy is decided by and enforced by C2K.
- All users must keep passwords private and should not permit others to use their log on id.
- The ICT technician should be informed if a user forgets their password or cannot access their C2K account.

ICT Hardware and Software

- No personally owned applications or software packages should be installed on to school ICT equipment;

Email

- Filtered email services for students and staff are provided by C2K. No other email service is to be used in school.

Mobile Phones

- Students should adhere to the school rules and guidelines regarding mobile phone use in school.

Copyright

- Students are taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Viruses and removable Data Storage Devices

- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks.

BYOD

- A separate BYOD policy is in place regulating 6th form use of personal computing devices. A copy is available from the school web site.