E-Safety Policy

Ferryhill Business and Enterprise Board of Governors have approved this core e-Safety Policy which will be used to educate and protect students.

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications, publishing and the appropriate use of personal data. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The safe and effective use of the Internet is an essential life-skill, required by all. However, unmediated Internet access brings with it the possibility of placing users in embarrassing, inappropriate and even dangerous situations. The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Children and young people must also learn that publishing personal information could compromise their own security and that of others.

The previous Internet Policy has been extensively revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

<u>End to End e-Safety</u>

E-Safety depends on effective practice at a number of levels:

 Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

 Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

 Safe and secure broadband from Durham ICT Services including the effective management of the inhouse Lightspeed filtering.

School e-safety policy

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Bullying and for Child Protection.
 The school e-Safety Co-ordinator role is part of the Child Protection and Safeguarding roles of key members of the Leadership Team.
 Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by Senior Management and approved by Governors.
 The e-Safety Policy and its implementation will be reviewed annually.
 The e-Safety Policy was revised by: Kevin Brennan and Mark Webb

1.2 Teaching and Learning

1.2.1 Why Internet use is important

 The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
 Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2.2 Internet use will enhance learning

 The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Levels of access will vary depending on the Key Stage of the students.
 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.3 Pupils will be taught how to evaluate Internet content

 As a school we should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
 Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

1.2.4 – Teaching and Learning

E-safety covered in IT lessons

Year 7
Internet research (covering copyright, safety online, recognising reliable sites, validity, accuracy, etc)
Creating a strong password and importance of keeping it safe
Chatroom safety
Netiquette
General e-safety issues

1.2.4 – Teaching and Learning continued..

E-safety covered in IT lessons

Year 8
Scenario based e-safety lessons – using CEOP videos

Year 9
Scenario based e-safety lessons – using CEOP videos

Year 10
Cyber stalking – videos and discussion.

1.3 Managing Internet Access

1.3.1 Information system security
 School ICT systems capacity and security will be reviewed regularly.
 Virus protection will be installed and updated on a regular basis.
 Users are responsible for their own logon details and should reset passwords if they believe their account has been compromised at the earliest opportunity.

1.3.2 E-mail
 Pupils may only use approved e-mail accounts on the school system. Electronic communication between staff and students should only take using the school provided e-mail system.
 Pupils must immediately tell a teacher if they receive an offensive e-mail.
 Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
 E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
 The forwarding of chain letters is not permitted.

1.3.3 Published content and the school web site
 The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published.
 The Network Manager or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

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

1.3.5 Social networking and personal publishing

 School will block/filter access to social networking sites both on Networked PC's and via the Schools wireless for all staff and students.
 Newsgroups will be blocked unless a specific use is approved.
 Pupils will be advised never to give out personal details of any kind which may identify them or their location.
 Pupils must not place personal photos on any social network space.
 Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
 Regular Facebook safety sessions will be held for Students and Parents including information how to protect your social presence.

1.3.6 Managing filtering

 If staff or pupils discover an unsuitable site, it must be reported via IT Support.
 The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing videoconferencing

 IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
 Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
 Videoconferencing will be appropriately supervised for the pupils' age.

1.3.8 Managing emerging technologies

 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
 Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

1.3.9 Protecting personal data

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

1.4 Policy Decisions

1.4.1 Authorising Internet access

 All staff must read and sign the 'Staff Acceptable Usage Policy before using any school ICT resource. This will be shown the first time a member of staff logs onto the System as well as whenever a change to the policy has been made.
 The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
 Secondary students must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy upon logon to the System. Parents will be asked to sign and return a consent form at the start of the academic year.

1.4.2 Assessing risks

 The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School cannot accept liability for the material accessed, or any consequences of Internet access.
 The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

1.4.3 Handling e-safety complaints

 Complaints of Internet misuse will be dealt with by a senior member of staff.
 Any complaint about staff misuse must be referred to the Headteacher.
 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
 Pupils and parents will be informed of the complaints procedure via the schools website and upon request.
 Discussions will be held with the Police and Durham LA Safeguarding team to establish procedures for handling potentially illegal issues.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

 e-safety rules will be posted in all networked rooms.
 Pupils will be informed that network and Internet use will be monitored.

1.5.2 Staff and the e-Safety policy

 All staff will be given the School e-Safety Policy and its importance explained.
 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
 Staff that manage filtering systems or monitor ICT use will have clear procedures for reporting issues.

1.5.3 Enlisting parents' support

 Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.

APPENDICES

FERRYHILL BUSINESS AND ENTERPRISE COLLEGE

GUIDANCE FOR SAFER WORKING PRACTICE
FOR ADULTS WORKING WITH
CHILDREN AND YOUNG PEOPLE IN THE USE OF NEW TECHNOLOGIES

Rationale

In order to make best use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that e-safety risks are posed more by behaviours and values than the technology itself. It is therefore imperative that staff working in schools act as role models in this area and must therefore ensure that they establish safe and responsible online behaviours at all times. This means working to local and national guidelines on acceptance user policies. These detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. VLE's are now widely established and clear agreement by all parties about acceptable and responsible use is essential.

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communication is transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretations of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. E-mail or text communication between an adult and a young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

All forms of student communication should be via Internal e-mail systems (using the provided @fbec.co.uk addresses) and should only be used in accordance with the school policy. As a reminder all internet and e-mail activity is actively monitored at all times and investigations could take place on the request of the schools Headteacher / Governing Body. Therefore, you are reminded that there is no expectation of privacy in the use of school computers, networks and/or internet services.

Staff must seek authorization from their Subject Leader and / or the schools Network Manager for access to external websites which are to be used in lessons or as part of schemes of work, as well as those that are made available via the Learning Gateway subject areas to students. Certain websites may be deemed unsuitable for educational use and will therefore be filtered from access within school due to the potential inappropriateness of the content therein.

Protocol for FBEC Staff

This means that all staff should:

 ensure that personal social networking sites such as Facebook are set as private and current or ex students are never listed as approved contacts; access to all social networking sites are not permitted within school.
 never browse or access social networking sites of students;
 not give their personal contact details to students, including their mobile telephone number, address or personal e-mail address;
 only make contact with children for professional reasons and in accordance with any school policy;
 take responsibility for their own use of new technologies, making sure that they use technology safely, responsibly and legally.
 report any known misuse of technology, including the unacceptable behaviour of others.

Photography and Videos

Rationale

Working with pupils may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of pupils. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.

Staff need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.

It is not appropriate for staff to take photographs of children for their personal use. It is recommended that when using a photograph the following guidance should be followed:

 if the photography is used, avoid naming the pupil, avoid using full names and to use “Pupil A” or “Stephen D” as an example
 if the pupil must be named, avoid using their photograph
 schools should establish whether the image will be retained for further use as part of the Data Protection Act
 Images should be securely stored and used only by those authorised to do so.

Protocol for FBEC'S Staff

This means that staff should:
 be clear about the purpose of the activity and about what will happen to the images when the activity is concluded
 be able to justify images of children in their possession
 avoid making images in one to one situations or which show a single child with no surrounding context
 ensure that the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed
 only use equipment provided or authorised by the school
 report any concerns about any inappropriate or intrusive photographs found
 always ensure they have explicit parental permission to take and/or display photographs either around school or via external media – websites, newspapers, local authority publications etc

This means that staff should not:
 display or distribute images of children unless they have consent to do so from parents/carers
 use images which may cause distress
 use personal mobile telephones or any other similar devices to take images of children
 take images "in secret" or taking images in situations that may be construed as being secretive
 under any circumstances retain images of students on personal memory pens, laptops or computers at home

Ferryhill Business and Enterprise College

Staff Acceptable Usage Policy

Internet Acceptable Use Policy
For the purposes of this document the 'internet' is defined as; web services, chat rooms, bulletin boards, newsgroups, peer to peer file sharing and instant messaging software.

General Principles
 Use of the Internet by School staff is permitted and encouraged where such use is supports the goals and objectives of the School.
 Use of Internet is monitored for security and/network management reasons. Users may also be subject to limitations on their use of such resources.

Unacceptable Use or Behaviour:
It is unacceptable to;
 Visit Internet sites that contain obscene, hateful or other objectionable materials.
 Make or post indecent remarks, proposals or materials on the Internet including racist or sexist jokes and defamatory comments.
 Download any software or electronic files without the use of virus protection measures that have been installed by a member of ICT Support.
 Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network

Users should:
 If you become aware that there has been unauthorised access to your computer account, you must raise it immediately with a member of ICT Support because of the implications for the security of School, and personal data.
 Record any instances where you have accessed inappropriate sites by accident. For example this may be through mistyping an address or spam email link.
 Data of a personal nature must only be stored on school approved encrypted memory sticks or encrypted staff laptops.
 Staff workstations must be locked or logged whilst unattended, so as to protect the data and to allow other members of staff to use the computer.
The School accepts that the use of the Internet is an extremely valuable business, research and learning tool. However misuse of such a facility can have a detrimental effect on other users. As a result, the School monitors;
 The volume of internet and network traffic The internet sites visited
 The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Staff e-mail Acceptable Usage Policy

Email Acceptable Use Policy
This Email Acceptable Use Policy (AUP) applies to all School staff.
General Principles
 Use of email by School employees is permitted and encouraged where such use is suitable for school purpose and supports the goals and objectives of the School. Users must follow the e-mail etiquette policy in sending any emails both internally and externally.
 School email accounts are to be used for School business. Limited personal use is considered acceptable.
 Use of email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources
 Email messages are treated as potential corporate messages of the school.
 The School reserves the right to redirect the email of staff that have left for legitimate business purposes. Users are responsible for ensuring personal emails are stopped.

Unacceptable Use or behaviour:
It is unacceptable to;
 Solicit emails that are unrelated to school activities or for personal gain.
 Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
 Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the School, or the School itself.
 Waste time on non-School business.

Users should:
 Keep emails brief and use meaningful subject lines.
 Re-read messages before sending to check for clarity and to make sure that they contain nothing which will make the school liable.
 Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email.
 Archive effectively - use folders and delete any messages you no longer need.
 Never reply to spam.
 Avoid using email for sensitive or emotional messages or offensive content.
 Staff Emails are a form of school communication and therefore should be drafted with the same care as letters.
 Users should be careful when replying to emails previously sent to a group.

Monitoring
The School accepts that the use of email is an extremely valuable business, research
and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the school's public profile. As a result;
 The School maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation
 The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Ferryhill Business and Enterprise College

Student Acceptable Use Policy

e-mail

Email Acceptable Use Policy
This Email Acceptable Use Policy (AUP) applies to all Students.

General Principles
 Use of email by Students is permitted and encouraged where such use is suitable for school purposes and supports the goals and objectives of the School. Users must follow this e-mail etiquette policy in sending any e-mails both internally and externally.
 School email accounts are to be used for School business. Limited personal use is considered acceptable.

General Principles continued…

 Use of email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources
 The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. For example; the Police can have a right of access to recorded data in pursuit of a crime.

Unacceptable Use or behaviour:
It is unacceptable to;
 Solicit emails that are unrelated to school activities or for personal gain
 Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person
 Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the School, or the School itself
 Waste time on non-School related activities

Users should:
 Keep emails brief and use meaningful subject lines
 Re-read messages before sending to check for clarity and to make sure that they contain nothing which will make the school liable
 Understand how to use - and don't mismanage - CC and BCC: only CC in people that really need to receive the email
 Archive effectively - use folders and delete any messages you no longer need.
 Never reply to spam
 Avoid using email for sensitive or emotional messages or offensive content
 Users should be careful when replying to emails previously sent to a group.

Monitoring
The School accepts that the use of email is an extremely valuable research and learning tool. However misuse of such a facility can have a detrimental effect on other users and potentially the school's public profile. As a result;
 The School maintains the right to access user email accounts in the pursuit of an appropriately authorised investigation
 The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Internet

Internet Acceptable Use Policy
For the purposes of this document the ‘internet’ is defined as; web services, chat rooms, bulletin boards, newsgroups, peer to peer file sharing and instant messaging software.
General Principles
 Use of the Internet by Students is permitted and encouraged where such use supports the goals and objectives of the School.
 Use of Internet is monitored for security and/network management reasons. Users may also be subject to limitations on their use of such resources.

Unacceptable Use or behaviour:

It is unacceptable to;

 Visit Internet sites that contain obscene, hateful or other objectionable materials

 Make or post indecent remarks, proposals or materials on the Internet including racist or sexist jokes and defamatory comments.

 Download any software or electronic files

 Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network

Users should:

 If you become aware that there has been unauthorised access to your account, you must raise it immediately with a member of ICT Support because of the implications for the security of School, and personal data.

 Record any instances where you have accessed inappropriate sites by accident. For example; this may be through mistyping an address or spam email link.

 Log out of the computer when you have finished

The School accepts that the use of the Internet is an extremely valuable business, research and learning tool. However, misuse of such a facility can have a detrimental effect on other users. As a result, the School monitors;

 The volume of internet and network traffic The internet sites visited

 The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Ferryhill Business & Enterprise College
Merrington Road
Ferryhill
Co Durham
DL17 8RW