Magherafelt Learning Partnership

E-Safety Policy

Safeguarding pupils, staff and college in a digital world

This e-Safety policy was created by the:-
Magherafelt Learning Partnership ICT Subgroup

The following groups were consulted during the creation of this policy:-

Staff

Parents/guardians

Pupils

NEELB CASS Team

C2k Support Staff

Policy was completed in November 2011

Policy was approved by the Board of Governors of
St. Pius X College on December 2011

The policy is due for review no later than: September 2016

St. Pius X College's e-safety Coordinator is Mrs. E Mc Stocker

Table of Contents

Acknowledgement

This document based on original documents by '**Yorkshire & Humber Grid for Learning'** and '**London Grid for Learning'** was produced by the ICT Subgroup of the Magherafelt Learning Partnership.

Introduction

This e-safety policy recognises our commitment to e-safety and acknowledges its part in the college's overall Safeguarding Policies and Procedures. It shows our commitment to meeting the requirements to safeguard and promote the welfare of pupils as outlined in Articles 17 & 18 of the Education and Libraries (Northern Ireland) Order 2003.

The whole college community can benefit from the opportunities provided by the Internet and other technologies used in everyday life and support the overarching goal of the Empowering Colleges Strategy (March 2004) ***"That all young people should be learning, with, through and about the use of digital and online technologies".***

This e-safety policy identifies the risks involved in using the Internet and the wide range of new technologies available. It sets out the steps the college is taking to avoid these risks or to minimise such risks where total elimination is not achievable. The college is committed to developing a set of safe and responsible behaviours by all members of the college community that will enable us to avoid/reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in the Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to e-safety we also recognise our obligation to implement a range of security measures to protect the college network and facilities from attack, compromise and inappropriate use and to protect college data and other information assets.

For the purposes of clarity and consistency throughout this document the lead person in college on e-Safety is called the e-Safety Coordinator**.**

The following local and national guidance is acknowledged in the formation of this e-Safety policy:-

1. Department of Education Circular Number 2007/1

2. Empower Colleges Strategy (March 2004)

3. British Educational & Communications Technology Agency (Becta)

4. Childnet International

5. Child Exploitation and Online Protection Centre

6. DCSF - Department for Children Colleges and Families guidance

Responsibilities of the College Community

E-Safety is the responsibility of the whole college community and everyone has their part to play in ensuring that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

2.1 Senior Management Team Responsibilities:

- Appoint a person (the e-Safety coordinator) to take responsibility for e-Safety and support them in their work
- Provide clear channels of communication for the e-Safety coordinator to liaise with the Senior Management Team
- Liaise with the college's Board of Governors by having an e-Safety regularly on the agenda of Board meetings.
- Ensure that access to the college ICT system is as safe and secure as reasonably possible.
- Ensure that servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access.
- Make appropriate resources, training and support available to all members of the college community to ensure they are able to carry out their roles effectively with regard to e-Safety
- Ensure that a comprehensive e-Safety education programme is in place and delivered to all staff, pupils and parents
- Ensure that the college's Child Protection Officer(s) have training geared to meeting the challenges presented by the wide use of the new technologies
- Develop and promote an e-Safety culture within the college community
- Ensure adequate technical support is in place to maintain a secure ICT system
- Ensure policies and procedures are in place to ensure the integrity of the college's information and data assets
- Ensure that procedures are in place to prevent personal data being sent over the Internet unless such data is encrypted or otherwise made secure
- Ensure that all users are informed that college equipment must not be used to view and transmit inappropriate material. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer".
- Ensure that all staff and pupils agree to the Acceptable Use Policy and that new staff have e-Safety included as part of their induction procedures
- Receive and regularly review e-Safety incident logs; ensure that the correct procedures are followed should an e-Safety incident occur in college and review incidents to see if further action is required
- Ensure that the college offers opportunities for parents/guardians to increase their knowledge of how ICT is used by their children and the e-safety issues arising from that use
- Ensure that only technical staff are permitted to download and install software onto the C2K network.
- Take ultimate responsibility for the e-Safety of the college community

2.2 e-Safety Coordinator Responsibilities

- Promote an awareness and commitment to e-Safety throughout the college
- Be the first point of contact in college on all e-Safety matters
- Create and maintain e-Safety policies and procedures working with other e-Safety coordinators within the Magherafelt Learning Partnership
- Develop an understanding of current e-Safety issues, guidance and appropriate legislation
- Ensure delivery to all staff and pupils an appropriate level of training in the **full range of e-Safety issues** identified in this policy
- Ensure that e-Safety education is in place and embedded across the curriculum
- Ensure that staff and pupils know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable
- Liaise with technical staff and C2k for the blocking of inappropriate websites, social network sites and other unsuitable digital material
- Ensure that e-Safety is promoted with parents/guardians and advice given as to how they can support their children should they become victims through the Internet and other technological malpractice
- Ensure that all staff and pupils understand the contents of the appropriate Acceptable Use Policy and that it is signed, returned and filed securely
- Ensure that any person who is not a member of college staff , who makes use of the college ICT equipment in any context, is made aware of the appropriate Acceptable Use Policy
- Ensure that all members of the college community understand the consequences of not following the regulations set in the Acceptable Use Policies which they have signed
- Monitor, report and advise on e-Safety issues to the Senior Management Team and Governors as appropriate
- Advise the Senior Management Team of future training needs to meet the requirements presented by the role of e-Safety Coordinator
- Liaise with the Local Educational Authority and other relevant agencies as appropriate
- Ensure an e-Safety incident log is kept up-to-date
- Ensure that Good Practice Guides for e-Safety are displayed in classrooms and around the college

2.3 Responsibilities of all Staff

- Read, understand and help promote the college's e-Safety policies and guidance
- Read, understand and adhere to the Staff AUP
- Develop and maintain an awareness of current e-Safety issues and legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times
- Take responsibility for ensuring the safety of sensitive college data and information

- Be responsible for, or assist with the delivery of the e-Safety education programme to pupils, ensuring that pupils fully understand the requirements of the Pupil AUP and that it is duly signed.
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Foster a 'No Blame' culture so that pupils feel able to report any cyber-bullying, 'grooming' abuse or receipt of inappropriate digital materials
- Be aware of how to advise pupils who receive uninvited/unwelcome attention or are presented with inappropriate materials as a result of their use of the new technologies
- Inform and periodically remind pupils that their use of the Internet is monitored
- Remind pupils not to share their password with any other person
- Encourage pupils to keep back-ups of all their work and to name their USB memory pens so that ownership can be established in the event of loss
- Preview all websites which they intend to incorporate into their teaching or use only sites accessed from managed 'safe' environments such as the college VLE
- Be vigilant when pupils are conducting investigative searches with search engines such as Google
- Respect the feelings, rights, values and intellectual property of others in their use of technology in college and at home
- Report all e-Safety incidents which occur in the appropriate log and/or to their line manager
- Report any failure of the filtering systems to the college Network manager and C2k

2.4 Responsibilities of Pupils

- Read, understand and adhere to the Pupil AUP and follow all safe practice guidance
- Take responsibility for their own and each others' safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of college
- Reminded not to share their password with any other person
- Reminded to name their USB memory pen so that ownership can be established in the event of loss
- Reminded to take back-up copies of any files which they generate
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in college and at home
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- Report all e-Safety incidents to appropriate members of staff
- Discuss e-Safety issues with family and friends in an open and honest way

2.5 Responsibilities of Parents and Guardians

- Help and support the college in promoting e-Safety
- Read, understand and promote the Pupil AUP with their children
- Discuss e-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Be aware of those sites which can offer advice and support to children who receive uninvited/unwelcome attention or are presented with inappropriate materials as a result of their use of the new technologies
- Consult with the college if they have any concerns about their child's use of technology

2.6 Responsibilities of Technical Staff (ICT Technician)

- Ensure that servers, workstations and other hardware and software are kept updated as appropriate.
- Ensure that a firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date by C2k.
- Check that staff have virus protection installed on all laptops used for college activity.
- Maintain the filtered broadband connectivity through C2k
- In conjunction with C2k immediately remove access to any website considered inappropriate by staff or pupils
- Ensure that only approved or checked webcam sites are available for staff /pupil use
- Keep up-to-date with C2k services and policies
- Ensure appropriate technical steps are in place to safeguard the security of the college ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- At the request of the Senior Management Team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any e-Safety-related issues that come to their attention to the e-Safety coordinator and/or Senior Management Team
- Ensure that procedures are in place for new users and leavers to be correctly added to and removed from all relevant electronic systems
- Ensure that suitable access arrangements are in place for any external users of the college's ICT equipment
- Ensure that any administrator or master passwords for college ICT systems are kept secure and available to at least two members of staff, e.g. head teacher and C2K Network Manager.
- Ensure that the wireless network is protected by a secure log on which prevents unauthorised access. New users can only be given access by named individuals e.g. a member of technical support.
- Liaise with C2K and others on e-Safety issues

2.7 Responsibility of any external users of the college systems e.g. adult or community education groups

- Take responsibility for liaising with the college on appropriate use of the college's ICT equipment and Internet
- Ensure that participants are trained in the requirements set out in the Temporary Staff/Visitors AUP and that this policy has been signed by the participants

2.8 Responsibilities of Governing Body

- Read, understand, contribute to and help promote the college's e-Safety policies and guidance as part of the college's overarching safeguarding procedures
- Support the work of the college in promoting and ensuring safe and responsible use of technology in and out of college, including encouraging parents to become engaged in e-Safety awareness
- Ensure appropriate funding and resources are available for the college to implement their e-Safety strategy

3.1 Learning and Teaching

The key to developing safe and responsible behaviours online for everyone within the college community lies in effective education. The Internet and other technologies are embedded in pupils' lives, not just in college but outside as well, and the college has a duty to help prepare pupils to benefit safely from the opportunities that these present.

The college will:-

- Develop an environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensure pupils and staff, know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensure pupils and staff know what to do if there is a cyber-bullying incident; behaviour
- Ensure all pupils know how to report abuse;
- Have a clear, progressive e-safety education programme throughout all Key Stages. Teach pupils a range of skills and behaviours appropriate to their age and experience, such as:
    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site/page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines/web sites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - to understand how search engines work;
    - to understand 'Netiquette' behaviour when using an online environment/email, i.e. be polite, no offensive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract unwelcome attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
- Ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright/intellectual property rights;
- Ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming/gambling;
- Ensure staff know how to encrypt data where confidentiality demands such action and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- Makes training available annually to staff on the e-safety education program;

3.2 Internet Access

Web filtering of internet content is provided by C2K. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. Notices are posted in classrooms and around college as a reminder.

The college decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the college who may be granted a temporary login.

All users are provided with a login appropriate to their key stage or role in college. Pupils are taught about safe practice in the use of their login and passwords.

All users should only be using the Internet in response to a legitimate articulated need.

Staff are given appropriate guidance on managing access to laptops which are used both at home and college and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to college systems is covered by specific agreements and is never granted to unauthorised third party users.

3.3 Using the Internet

The college provides the internet to:-

- Support curriculum development in all subjects;
- Facilitate and encourage independent learning and research by pupils;
- Support the professional work of staff as an essential professional tool;
- Enhance the college's management information and business administration systems;
- Enable electronic communication and the exchange of curriculum and administration data with the Department of Education, the Examination Boards and others;

Users are made aware that they must take responsibility for their use of, and their professional conduct whilst using, the college ICT systems or a college provided laptop or device and that such activity can be monitored and checked.

All users of the college ICT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around college.

*Additional guidance for staff and pupils is included in the **MLP Electronic Communications Guidance for Staff** and this is included as part of the college's e-Safety Policy.*

3.4 Using email

Email is regarded as an essential means of communication and the college provides all members of the college community with an e-mail account for college-based communication. Communication by email between staff, pupils and parents will only be made using the college email account and should be professional and related to college matters only. E-mail messages on college business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the college is maintained. There are systems in place for storing relevant electronic communications which take place between college and parents.

C2k operates an appropriate educational filtered Internet-based email system for colleges.

In the college context e-mail should not be considered private and the college reserves the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

As part of the curriculum pupils are taught about safe and appropriate use of email. Pupils are informed that misuse of email will result in a loss of privileges.

Responsible use of personal web mail accounts by staff may be permitted.

All users are reminded that sending threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the telecommunications Act (1984)

*Additional guidance for staff and pupils is included in the **MLP Electronic Communications Guidance for Staff** and this is included as part of the college's e-Safety Policy.*

3.5 Using images, Video and Sound

It is recognised that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

All parents/carers are asked to sign an agreement about taking and publishing photographs and video of their children and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff or other visitors to college never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

*Additional guidance for staff and pupils is included in the **MLP Electronic Communications Guidance for Staff** and this is included as part of the college's e-Safety Policy.*

3.6 Using Video Conferencing and other Online Meetings

Video conferencing is used to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. Staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Pupils do not operate video conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and pupil(s) which takes place outside college or whilst the member of staff is alone is always conducted with the prior knowledge of the head teacher or line manager and respective parents/carers.

Additional guidance for staff and pupils is included in the ***MLP Electronic Communications Guidance for Staff*** *and this is included as part of the college's e-Safety Policy.*

3.7 Publishing Content Online

(a) College Website:

The college maintains editorial responsibility for any college initiated web site or virtual learning platform content to ensure that content is accurate and the quality of presentation is maintained. The college maintains the integrity of the college web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the college address, e-mail and telephone number. Contact with staff is though the receptionists in the college office.

Identities of pupils are protected at all times. Photographs of identifiable individual pupils are not published on the web and group photographs do not have a name list attached. The college obtains permission from parents for the use of pupils' photographs.

(b) VLE, Blogs, Wikis, Podcasts, Social Network Sites

As part of the curriculum pupils are encouraged to create online content. Pupils are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Blogging, podcasting and other publishing of online content by pupils will take place within the college virtual learning platform or other media selected by the college. Pupils will only be allowed to post or create content on sites where members of the public have access, when this is part of a college related activity. Appropriate procedures to protect the identity of pupils will be followed.

All reasonable steps are taken to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

(c) Online Material Published outside the College:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside college as they are in college.

Material published by pupils, governors and staff in a social context which is considered to bring the college into disrepute or considered harmful to, or harassment of another pupil or member of the college community will be considered a breach of college discipline and treated accordingly.

*Additional guidance for staff is included in the **MLP Electronic Communications Guidance for Staff** and this is included as part of the college's e-Safety Policy.*

3.8 Using Mobile Phones

Multimedia and communication facilities provided by a mobile phone can provide beneficial opportunities for pupils. However their use in lesson time will only be with permission from the teacher.

College mobile phones or similar devices with communication facilities used for curriculum activities are set up appropriately for the activity. Pupils are taught to use them responsibly.

Where required for safety reasons in off-site activities, a college mobile phone is provided for contact with pupils, parents or the college. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Unauthorised or secret use of a mobile phone or other electronic device, to record voice, pictures or video is forbidden. Unauthorised publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of college discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

*Additional guidance for staff and pupils is included in the **MLP Electronic Communications Guidance for Staff** and this is included as part of the college's e-Safety Policy.*

3.9 Using other technologies

As a college we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-Safety point of view.

We will regularly review the e-Safety policy to reflect any new technology that the college proposes to use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behavior to those outlined in this document.

4.1 Protecting College Data and Information

The college recognises its obligation to safeguard staff and pupils' personal data including that which is stored and transmitted electronically. Practices and procedures to ensure that the college meets this basic obligation are regularly reviewed.

The college is a registered Data Controller under the Data Protection Act 1998 and will comply at all times with the requirements of that registration.

Pupils are taught about the need to protect their own personal data as part of their e-Safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the college's management information systems holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside college
- When the college disposes of old computers and other equipment we take due regard for destroying information which may be held on them
- Data is transmitted securely and sensitive data is not sent via email unless encrypted
- Remote access to computers is by authorised personnel only
- The college has full back up and recovery procedures in place for college data
- Where sensitive staff or pupil data is shared with other people who right of access to the information, for example Governors, Social Services, the material is labeled appropriately to remind them of their duty to keep it secure and to securely destroy any spare copies

5.1 Dealing with e-Safety Incidents

All e-Safety incidents are recorded in the College e-Safety Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the college's normal disciplinary procedures.

In situations where a member of staff is made aware of a serious e-Safety incident, concerning pupils or staff, they will inform the e-Safety coordinator, their line manager or head teacher who will then respond in the most appropriate manner.

Instances of **cyberbullying** will be taken very seriously by the college and dealt with using the college's anti-bullying procedures. College recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Incidents which create a risk to the security of the college network, or create an information security risk, will be referred to the college's e-Safety coordinator and technical support and appropriate advice sought and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches college policy then appropriate sanctions will be applied. The college will decide if parents need to be informed if there is a risk that pupil data has been lost.

The college reserves the right to monitor college equipment used off-site and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on a computer, then the incident will be referred to the Designated Teacher and the Principal. The Child Protection Procedures of the college will be followed.

5.2 Activities consistent with unacceptable (possibly illegal) conduct

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

5.3 Activities likely to result in disciplinary action:

- any online activity by a member of the college community which is likely to adversely impact on the reputation of the college
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at college or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using college or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the college into disrepute
- attempting to circumvent college filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission

- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data protection Act, revised 1988

5.4 Normally unacceptable activities which may be allowed e.g. as part of planned curriculum activity or as system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another person to login using your account
- accessing college ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Appendix A

Extracts from:

Guidance for Safer Working Practice for Adults who work with Children and Young People. DCSF January 2009

Section 12 Communication with Children and Young People *(including the Use of Technology)*

Communication between children 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 communications are transparent and open to scrutiny.

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

Internal e-mail systems should only be used in accordance with the organisation's policy.

Organisations should therefore have a communication policy which specifies acceptable and permissible modes of communication:-

This means that adults should:

- *not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites*
- *only use equipment e.g. mobile phones, provided by organisation to communicate with children, making sure that parents have given permission for this form of communication to be used*
- *only make contact with children for professional reasons and in accordance with any organisation policy*
- *recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible*
- *not use internet or web-based communication channels to send personal messages to a child/young person*
- *ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum*

Section 27 Photography and Videos

Working with children and young people 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 children and young people. Informed written consent from parents/guardians 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.

Adults 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 adults to take photographs of children for their personal use.

Adults should therefore:-

- *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 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 organisation*
- *report any concerns about any inappropriate or intrusive photographs found*
- *always ensure they have parental permission to take and/or display photographs*

Adults should not therefore:-

- *display or distribute images of children unless they have consent to do so from parents/carers*
- *use images which may cause distress*
- *use mobile telephones to take images of children*
- *take images 'in secret', or taking images in situations that may be construed as being secretive.*

Section 28 Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to their organisation to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Organisations and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

This means that organisations should:-

- *have clear e-safety policies in place about access to and use of the internet*

- *make guidance available to both adults and children and young people about appropriate usage.*

This means that adults should:-

- *follow their organisation's guidance on the use of IT equipment*
- *ensure that children are not exposed to unsuitable material on the internet*
- *ensure that any films or material shown to children and young people are age appropriate*

Sexual Offences Act 2003 and Grooming

Section 15 of the Sexual Offences Act 2003 makes it an offence for a person (A) aged 18 or over to meet intentionally, or to travel with the intention of meeting a child under 16 in any part of the world, if he has met or communicated with that child on at least two earlier occasions, and intends to commit a "relevant offence" against that child either at the time of the meeting or on a subsequent occasion. An offence is not committed if (A) reasonably believes the child to be 16 or over.

The section is intended to cover situations where an adult (A) establishes contact with a child through for example, communications on the internet and gains the child's trust and confidence so that he can arrange to meet the child for the purpose of committing a "relevant offence" against the child.

The course of conduct prior to the meeting that triggers the offence may have an explicitly sexual content, such as (A) entering into conversations with the child about sexual acts he wants to engage him/her in when they meet, or sending images of adult pornography. However, the prior meetings or communication need not have an explicitly sexual content and could for example simply be (A) giving swimming lessons or meeting him/her incidentally through a friend.

The offence will be complete either when, following the earlier communications, (A) meets the child or travels to meet the child with the intent to commit a relevant offence against the child. The intended offence does not have to take place.

The evidence of (A's) intent to commit an offence may be drawn from the communications between (A) and the child before the meeting or may be drawn from other circumstances, for example if (A) travels to the meeting with ropes, condoms and lubricants.

Subsection (2) (a) provides that (A's) previous meetings or communications with the child can have taken place in or across any part of the world. This would cover for example (A) emailing the child from abroad, (A) and the child speaking on the telephone abroad, or (A) meeting the child abroad. The travel to the meeting itself must at least partly take place in England or Wales or Northern Ireland.

APPENDIX B

STAFF/PUPIL INFRINGEMENTS OF E-SAFETY POLICY

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of Senior Management.

(a) Pupils

PUPILS	
Category A Infringements	**Sanctions**
▪ Use of non-educational sites during lessons ▪ Unauthorised use of email ▪ Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends ▪ Use of unauthorised instant messaging / social networking sites	Referral to: • Class Teacher/Class Tutor • Year Head/Head of College • e-Safety Coordinator • Principal
Category B Infringements	**Sanctions**
▪ Continued use of non-educational sites during lessons after being warned ▪ Continued unauthorised use of email after being warned ▪ Continued unauthorised use of mobile phone (or other new technologies) after being warned ▪ Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups ▪ Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc ▪ Accidentally corrupting or destroying others' data without notifying a member of staff of it ▪ Accidentally accessing offensive material and not logging off or notifying a member of staff of it	Referral to: • Class Teacher/H.o.D. • Year Head/Head of College • e-Safety Coordinator • Principal • Removal of Internet access rights for a period of time • Removal of phone until end of college day • Contact with parents
Category C Infringements	**Sanctions**
▪ Deliberately corrupting or destroying someone's data, violating privacy of others ▪ Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) ▪ Deliberately trying to access offensive or pornographic material ▪ Any purchasing or ordering of items over the Internet ▪ Transmission of commercial or advertising material ***action by college:*** ***Technical support to filter out inappropriate websites (C2k)***	Referral to: • Class Teacher/H.o.D. • Year Head/Head of College • e-Safety Coordinator • Principal • Removal of Internet and or Learning Platform access rights for a period of time • Removal of equipment • Contact with parents
Category D Infringements	**Sanctions**
▪ Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned ▪ Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent ▪ Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 ▪ Bringing the college name into disrepute ▪ Use of mobile phone or other new technologies to take inappropriate/unauthorised images of staff or pupils ***action by college:*** ***Secure and preserve any evidence and inform the sender's email provider***	Referral to: • Principal • Contact with parents • Possible exclusion • Removal of equipment • Contact PSNI

STAFF/PUPIL INFRINGEMENTS OF E-SAFETY POLICY

(b) Staff

STAFF	
Category A Infringements (Misconduct)	**Sanctions**
▪ Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. ▪ Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. ▪ Not implementing appropriate safeguarding procedures. ▪ Any behaviour on the World Wide Web that compromises the staff member's professional standing in the college and community. ▪ Misuse of first level data security, e.g. wrongful use of passwords. ▪ Breaching copyright or license e.g. installing unlicensed software on network.	Referred to Line Manager/Principal ***Warning given***
Category B Infringements (Gross Misconduct)	**Sanctions**
▪ Serious misuse of, or deliberate damage to, any college computer hardware or software; ▪ Any deliberate attempt to breach data protection or computer security rules; ▪ Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; ▪ Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; ▪ Bringing the college name into disrepute. ***action by college:*** • ***The PC/Laptop is removed to a secure place to prevent further access;*** • ***Instigate an audit of all ICT equipment by an outside agency (C2k) to ensure that there is nor risk of pupils accessing inappropriate materials in college;*** • ***Identify the precise details of the material***	Referred to Principal/Governors. ***College disciplinary procedures are followed. Reported to DENI and PSNI***
Category C Infringements (Very Serious Misconduct)	**Sanctions**
▪ Child Pornography or other very serious misconduct ***Action by college:*** • ***On discovery of images no downloading or distribution of any images should be completed either internally or externally.*** • ***Computer left and not used by anyone until forensic examination and investigation is completed.*** • ***Details of persons having access to the computer to be available to allow a clear evidence trail to be established.***	Referred to Principal/Governors ***College disciplinary procedures are followed. Reported to DENI and PSNI and Children's Social Care services. Member of staff suspended potentially resulting in dismissal.***

Methodology for informing staff/pupils/parents of these procedures

- They will be fully explained and included within the college's e-Safety and Acceptable Use Policies. All staff will be required to sign the college's e-safety Policy Acceptable Use Policy;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-safety Acceptable Use Policy;
- The college's e-safety policy will be made available and explained to parents. Letter of explanation will be sent to parents/guardians;

- Information on reporting abuse/bullying etc will be made available by the college for pupils, staff and parents/guardians;
- Staff are issued with the ‘Action to be taken by staff in the event of an e-safety incident’ guide on e-safety incidents.

APPENDIX C

ACTION TO BE TAKEN BY STAFF IN THE EVENT OF AN E-SAFETY INCIDENT

Incident	Action by staff member
An inappropriate website is accessed **unintentionally** in college by a teacher or child	• Play the situation down by remaining calm; • Report to the Principal /e-Safety officer and decide whether to inform parents of any children who may have viewed the site; • Inform the College Network Manager and ensure the site is filtered; • Inform C2k • Report to Principal and e-Safety Officer
An inappropriate website is accessed **intentionally** by a child	• Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions; • Notify the parents of the child; • Inform the College Network Manager and ensure the site is filtered if need be. • Inform C2k. • Report to Principal and e-Safety Officer
An adult uses college ICT equipment inappropriately	• Ensure you have a colleague with you; do not view the misuse alone; • Report the misuse immediately to the Principal and ensure that there is no further access to the PC or laptop; • If the material is offensive but not illegal, the Principal should then: ○ Remove the PC to a secure place; ○ Instigate an audit of all ICT equipment by the colleges ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the college; ○ Identify the precise details of the material; ○ Take appropriate disciplinary action; ○ Inform Governors of the incident; • In an extreme case where the material is of an illegal nature: ○ Contact the local police and follow their advice; ○ If requested to remove the PC to a secure place and document what you have done. • Report to Principal and e-Safety Officer
A bullying incident directed at a child occurs through email or mobile phone technology either inside or outside college	• Advise the child not to respond to the message; • Refer to relevant policies including e-safety anti-bullying and apply appropriate sanctions if the perpetrator is another pupil at college; • Secure and preserve any evidence; • Inform the sender’s e-mail service provider; • Notify parents of the children involved; • Consider delivering a parent workshop for the college community; • Inform the police if necessary. • Report to Principal and e-Safety Officer
Malicious or threatening comments are posted on an internet site about a pupil or member of staff	• Inform and request the comments be removed if the site is administered externally. • Secure and preserve any evidence. • Send all the evidence to CEOP at http://www.ceop.gov.uk/contact_us.html. • Endeavour to trace the origin and inform police as appropriate • Report to Principal and e-Safety Officer
There is concern that a child’s safety is at risk because someone is suspected of using	• Report to and discuss with the named child protection officer in college and contact parents. • Advise the child on how to terminate the communication and save all evidence. • Contact CEOP at http://www.ceop.gov.uk/

communication technologies (eg social networking sites) to make inappropriate contact with the child.	• Consider the involvement police and social services. • Consider delivering a parent workshop for the college .community • Report to Principal and e-Safety Officer

APPENDIX D

SAFE HANDLING OF DATA GUIDE

INTRODUCTION

The aim of this guide is to raise awareness on safe handling of data, data security and roles and responsibilities. Following these principles will help prevent information from being lost or used in a way which may cause individuals harm/distress or the reputation of the college being damaged through loss of sensitive information.

Everybody in the college has a shared responsibility to secure any sensitive information which they use in their professional duties and all staff should be aware of the risks involved.

Setting Passwords	
Staff must	**Staff must not**
• follow C2k password policy • use a strong password (strong passwords are usually 8 characters or more and contain upper and lower case letters, as well as numbers and special characters) • make your password easy to remember, but hard to guess. • choose a password that is quick to type • use a mnemonic to help you remember your password • change your passwords if you think someone may have found out what they are • change your passwords on a regular basis	• share their passwords with anyone else • write their passwords down • use their work passwords for your own personal online accounts • save passwords in web browsers if offered to do so • use their username as a password • use names as passwords • email their password or share it in an instant message
Storing Personal, Sensitive, Confidential or Classified Information	
Staff must	**Staff must not**
• ensure removable media is purchased with encryption and store all removable media securely • securely dispose of removable media that may hold personal data • encrypt all files containing personal, sensitive, confidential or classified data • ensure hard drives from machines no longer in service are removed and stored securely or wiped clean so that data cannot be restored. (see section on disposal of ICT equipment ICT Acceptable Use Policy • ensure hard copies of personal data are securely stored and disposed of after use • ensure that documents containing sensitive or personal data are correctly labelled • ensure that hard copies of confidential data are securely transported and stored when removed from college	

Sending and Sharing Data	
Staff must	**Staff must not**
• be aware of who you are allowed to share information with. Check with your e-Safety Co-ordinator • ask third parties how they will protect sensitive information once it has been passed to them	• send sensitive information (even if encrypted) on removable media (USB memory drives, CDs, portable drives) if secure remote access is available • send sensitive information by email unless it is encrypted • place protective labels on outside envelopes, use an inner envelope if necessary. This means that people can't see from the outside that the envelope contains sensitive information • assume that third party organisations know how your information should be protected. • Send IEP's or other documents which contain a pupil's Unique Pupil Number (UPN)
Email and Messaging	
Staff must	**Staff must not**
• report any emails that are not blocked or filtered which are seriously offensive, threatening or possibly illegal. • report phishing emails to the organisation they are supposedly from • use their college's contacts or address book. This helps to stop email being sent to the wrong address • only use their college email account for any college business, not your personal account such as Yahoo or Hotmail • when sending an email put a security classification in the first line of the email. For emails to do with information about a pupil, for example, you need to put in **PROTECT – PERSONAL** on the first line of the email. The name of the individual is not to be included in the subject line and the document containing the information is encrypted. This provides additional security • be wary of links to websites in emails, especially if the email is unsolicited	• click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on • turn off any email security measures that their IT team has put in place or recommended • email sensitive information unless they know it is encrypted. Talk to their IT support for advice • try to bypass their college's security measures to access their email offsite, for example forwarding email to a personal account • reply to chain e-mails
Working Online	
Staff must	**Staff must not**
• make sure that you follow your college's policies on keeping your computers up-to-date with the latest security updates. Make sure that you keep any computers that you own up-to-date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from your IT support if you need help • only visit websites that are allowed by your college. Remember your college may monitor and record (log) the websites you visit • make sure that you only install software that your IT team has checked and approved • be wary of links to websites in emails, especially if the email is unsolicited	

• only download files or programs from sources you trust. If in doubt talk to your IT support • check that your college has an acceptable internet use policy and ensure that you follow it	
Laptops or Workstations	
Staff must	**Staff must not**
• make sure that only approved software is installed and shut down their laptop or workstation using the ‘Shut Down’ or ‘Turn Off’ option • try to prevent people from watching you enter passwords or view sensitive information • turn off and store your laptop securely, for example, if travelling, use your hotel room’s safe or temporarily lock in the boot of your car • use a physical laptop lock if available to prevent theft • lock your desktop when leaving your laptop or workstation unattended • make sure your laptop, if it is contains personal or sensitive data, is protected with encryption software • use good password practices eg never keep your ID and password details with your laptop • only download files or programs from trusted sources	• store remote access tokens with your laptop • leave your laptop unattended unless they trust the physical security in place • use public wireless hotspots. They are not secure. • leave their laptop in their car. If this is unavoidable, temporarily lock it out of sight in the boot • let unauthorised people use their laptop • use hibernate or standby
Working Onsite	
Staff must	**Staff must not**
• lock sensitive information away when left unattended • use a lock for your laptop to help prevent opportunistic theft • make backup copies and protect them the same as the originals	
Working Offsite	
Staff must	**Staff must not**
• only take offsite information you are authorised to do so and it is necessary. Ensure that it is protected offsite in the ways referred to above • wherever possible access information remotely instead of taking it offsite • be aware of your location and take appropriate action to reduce the risk of theft • try to reduce the risk of people looking at what you are working with • leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies) • ensure only authorised staff are allowed to remove data from the college’s premises	• write down or otherwise record any network access information. Any such information that is recorded must be kept in a secure place and disguised • disclose login IDs, PINs and other dial-up information to unauthorised users

APPENDIX E

USEFUL WEBSITES

Website	Contents of website	Target Audience
Children, ICT & e-Safety	Information for parents on e-safety	Parents/Guardians/Pupils
Young People, ICT & e-Safety	Information for parents on e-safety	Parents/Guardians/Pupils
SMILE	SMILE Posters	Colleges/Pupils
Childnet Guide 1	Guide for parents/teachers on social networking sites	Parents/Teachers
Childnet Guide 2	Range of leaflets/posters on e-safety in a number of different languages	Parents/Teachers/Pupils
KNOWITALL Powerpoint	Powerpoint presentation on plagarism	Pupils/Teachers
KNOWITALL Films/Powerpoints	Film/Powerpoints on cyberbullying/copyright	Pupils/Teachers/Parents
Kirklees Site	e-safety posters on a range of issues	Pupils
Safe Surfing Poster in English	Safe Surfing Poster in English	Pupils
Safe Surfing Poster in Text Language	Safe Surfing Poster in text Language	Pupils
Cyberbullying – a whole-college community issue	Guide document (10 pages) with advice and support mechanism for pupils subject to cyberbullying	Pupils/Teachers/Parents
Cyberbullying – Supporting College Staff	Guide document (10 pages) with advice on supporting staff subject to cyberbullying	Staff
CEOP	Child Exploitation and Online Protection Centre – report to for cases of child abuse	Pupils/Staff/Parents
Childnet Site – General	Range of e-safety resources	Pupils/teachers/parents
Kidsmart	Range of advice on staying safe when using digital technologies	Pupils/Teachers/Parents
Rules for being online	Family Agreement Rules for being online	Pupils/Parents
Guidance on Safe Computer Use	Guidance on seating, use of keyboard, mouse and positing of screen in computer use	Pupils/Staff
Guidance on Posture	Powerpoint on good posture in computer use	Pupils/Parents
Epilepsy Action	Advice on Photosensitive Epilepsy	Pupils/Parents/Staff

REPORTING ABUSE - Phone Numbers and Websites

Service Provider	Phone Numbers	Web addresses
O2 Mobile	08705214000	ncb@o2.com
Vodafone Mobile	191 from Vodafone phone; 08700700191 for Pay monthly customers; 08700776655 for Pay as You Go customers	
3 Mobile	Call 333 from a 3 phone or 08707330333	
Orange Mobile	Call 450 from an Orange phone; 07973100450 for Pay as You Go; 150 or 07973100150 for Pay Monthly	
T-Mobile Mobile	Call 150 on a T-Mobile or 08454125000	
Facebook	Click on 'Report Abuse' link	Facebook.com
MySpace	Click 'Contact MySpace' link at bottom of	http://uk.myspace.com

Piczo	Click 'Report Bad Content' at top of every member page. At bottom of the homepage and on the 'Contact Us' page there is a link to 'Report Abuse' page.	The 'report Abuse' page can be found at http://pic3.piczo.com/public/piczo2/piczoAbuse.jsp
Video-hosting sites	On 'YouTube' create an account, login, and 'flag content as inappropriate' under the video content itself.	www.youtube.com/t/terms under section 5C
Instant Messenger	In MSN click 'Help' tab, select 'Report Abuse' In Yahoo Messenger click 'Help' tab and select 'Report Abuse' option	http://support.com/default.aspx?mkt=en-gb

APPENDIX F

HEALTH & SAFETY

(a) Location and supervision of computers in colleges

- Internet access for pupils in colleges should be available on computers in highly-used areas of the colleges such as classrooms, libraries, study areas, computer laboratories and media-centres;
- Where practical pupils should always be allocated to the same computer;
- Computer screens should be visible to staff circulating in the area and pupils should be supervised at all times where possible;
- Staff supervising pupils in areas such as computer laboratories should constantly alter the route they taken around the laboratory during general supervision.

(b) Posture – Ergonomics

(i) Setting up the chair and sitting comfortably

- Adjust the seat height so that the elbows are roughly the same height as the keyboard;
- Once the chair is at the correct height make sure that the feet rest flat on the floor;
- Adjust the height of the backrest so that it supports the curve in the lower back;
- Adjust the angle of the backrest in relation to the seat to a comfortable position;
- If the seat pan tilts, adjust it to suit the posture chosen;
- If there are arm rests they should be adjusted to a height just below elbow level
- Always sit as close to the desk as possible when using the computer;
- Always sit in the chair and use the backrest to support the back;
- Vary the sitting position periodically and occasionally lean back and relax;
- Adjust the height of the screen at or just below eye level for a touch typist, slightly lower for a non-touch typist.

(ii) Using the Keyboard and Mouse

- Use a soft touch when typing
- Keep the wrists straight, don't bend them upwards, downwards or sideways when typing;
- Rest the arms while not typing but don't rest the soft inner part of the wrist where the pulse would be taken, on the wrist rest or table edge;
- Vary the fingers used if not a touch typist;
- Use a light touch when holding or depressing the mouse button(s);
- Do not bend the hands upwards or sideways at the wrist while using the mouse;
- Do not stretch to use the mouse;
- Ensure there is enough space to use the mouse comfortably.

(iii) Screen, Desk and Work Environment

- Ideally blinds, curtains use to be used to control reflected glare or contrast light;
- The screen should be cleaned periodically;
- Move the eyes rather than the head when reading information on the screen;
- The layout of items should be prioritized on the desk with those items most often used nearest to the typist;
- If using a document holder adjust it to the same height, slope and viewing distance as the screen. The typist should consider locating the screen to one side with the document holder directly in front;
- Ensure lighting levels in the room are sufficient to read the screen and any documents to be referred to;
- Take breaks before tiredness or discomfort is experienced.

(iv) Software

- Use easy to read fonts such as arial;
- Limit the number of colours used on screen;
- Use pastel background colours particularly if reflections are a problem on the screen being used;
- Reduce dependency on mouse inputs by using keyboard equivalents and shortcuts

Guidance on safe Computer Use and a powerpoint Guidance on Posture should be read in conjunction with the above

(c) Interactive Whiteboards and Projectors

- All interactive whiteboards and other data projectors if misused have the potential to cause eye injury
- No one should stare directly into the beam of the projector at any time;
- If entering the beam, users should not look towards the audience for more than a few seconds;
- Use of a laser pointer to avoid the need to enter the beam is highly recommended;
- Users should stand with their back to the projector beam if standing in it is unavoidable;
- Children should be supervised at all times when a projector is being used;
- Projectors should be located out of the sight line from the screen to the projector;
- The heights of interactive whiteboards should be carefully considered to prevent undue stretching and bending of users;
- Installation of Whiteboards should follow the electrical installation guidelines of the local authority which in most cases will be the BS7671 and NICEIC standards;
- It is important to note that projector power installations which are classed as temporary are subject to PAT testing (Portable Appliance Testing) under the Electricity at Work regulations 1989.

(d) Photosensitive Epilepsy

- Using a computer is unlikely to be problematic for people with photosensitive epilepsy as the screen flicker is higher than the rate that triggers epilepsy;
- To reduce the risk of epilepsy to an absolute minimum it is important to consider both the type of software and display screen;
- For more detailed advice consult the website Epilepsy Action

(e) Wi-Fi and Wireless Local Area Networks (WLAN)

General position

There is no consistent evidence to date that exposure to radio signals from Wi-Fi and WLANs adversely affects the health of the general population. The signals are very low power, typically 0.1 watt (100 milliwatts) in both the computer and the router (access point), and the results so far show exposures are well within the internationally-accepted guidelines from the International Commission on Non-Ionizing Radiation Protection (ICNIRP). Based on current knowledge and experience, radio frequency (RF) exposures from Wi-Fi are likely to be lower than those from mobile phones. Also, the frequencies used in Wi-Fi are broadly the same as those from other RF applications such as FM radio, TV and mobile phones.

On the basis of the published studies and those carried out in-house, the HPA sees no reason why Wi-Fi should not continue to be used in colleges and in other places. However with any new technology a sensible precautionary approach, as happened with mobile phones, is to keep the situation under review so that parents and others can have as much reassurance as possible. That is why Sir William Stewart, former chairman of the HPA, stated that it would be timely to carry out further studies as this new technology is rolled out. Based on this, the HPA announced on 12 October 2007 that it would be carrying out a systematic programme of research into WLANs and their use, to include measurements of exposures from Wi-Fi networks, in particular those in colleges.

For further guidance consult the Health Protection Agency Wi-Fi website and Health Protection Agency Report website