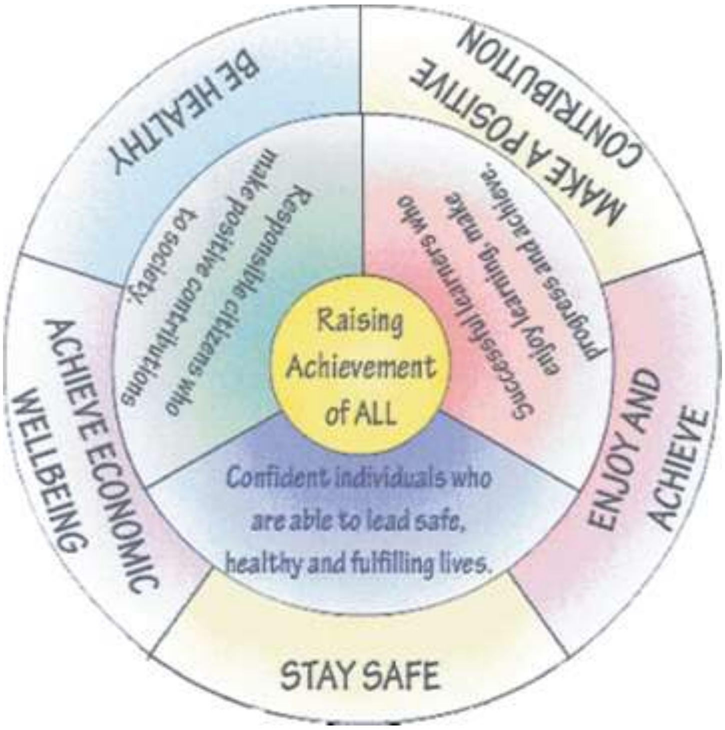
Hemsworth Arts and Community Academy

E Safety Policy

Updated
August 2013

The E-SAFETY policy supports the Academy aim by Raising Achievement of All.



BE HEALTHY
MAKE A POSITIVE CONTRIBUTION
ENJOY AND ACHIEVE
STAY SAFE
ACHIEVE ECONOMIC WELLBEING
Responsible citizens who make positive contributions to society.
Successful learners who enjoy learning, make progress and achieve.
Confident individuals who are able to lead safe, healthy and fulfilling lives.
Raising Achievement of ALL

- **Successful learners',** who enjoy learning, make progress and achieve.
- **Responsible Citizens',** who make positive contributions to society.
- **Confident individuals,** who are able to lead safe, healthy and fulfilling lives.

HACA IS COMMITTED TO SAFEGUARDING CHILDREN AND YOUNG PEOPLE. ANYONE WORKING IN COLLEGE, IN WHATEVER CAPACITY, IS EXPECTED TO SHARE THIS COMMITMENT.

HACA E-Safety Policy 2013

E-Safety Policy Content Details

1) Overview

This E-Safety policy was created by the E-Safety group consisting of:

Mr Stephen Foster (Assistant Principal)
Mr G Fee (Leader in New Technologies)
Mrs Cathyrn Clarke (Child Protection Officer)
James Kearton (Network Manager)

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

LT
Staff
Student Representative groups
Parent Representative Groups
Governors

The policy was completed on: 20th July 2013
The policy will be finally approved at the Local Governing Body (LGB) on 20th November
The policy is due for review no later than September 2014

2) Introduction

E-Safety is about enabling our community to benefit as much as possible from the opportunities provided by the Internet and the technologies we use in everyday life. It is not just about the risks, and how we avoid them, it is about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities.
An E-Safety policy allows HACA to demonstrate that we acknowledge E-Safety as an important issue for the HACA community. It also evidences the fact that we have made a considered attempt to embed E-Safety into our approach to learning using technology.
HACA's E-Safety policy will attempt to demonstrate how we have worked to achieve a balance between using technology to enhance learning and teaching, and putting appropriate safeguards in place.

3) General Responsibilities

Responsibilities of the HACA Community
E-Safety is the responsibility of the whole HACA Community and
everyone has their part to play in ensuring 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.

Responsibilities of the Leadership Team

- Develop and promote an E-Safety culture within the HACA community.
- Support the E-Safety / child protection Coordinator and Leader of New Technologies in their work.
- Make appropriate resources, training and support available to members of HACA community to ensure they are able to carry out their roles with regard to E-Safety effectively.
- Receive and regularly review E-Safety incident logs and be aware of the procedure to be followed should an E-Safety incident occur in HACA
- Take ultimate responsibility for the E-Safety of the HACA Community.

Responsibilities of the E-Safety Coordinator

- Promote an awareness and commitment to E-Safety throughout HACA.
- Be the first point of contact in HACA on all E-Safety matters.
- Lead on e-safety via the new technologies group.
- Create and maintain E-Safety policies and procedures.
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation.
- Ensure all members of staff receive an appropriate level of training in E-Safety issues.
- Ensure that E-Safety education is embedded across the curriculum.
- Ensure that E-Safety is promoted to parents and carers.
- Liaise with the local authority, WCAT and other relevant agencies as appropriate.
- Monitor and report on E-Safety issues to the new technologies group and SLT as appropriate
- Ensure an E-Safety incident log is kept up-to-date. Logs are to be kept using records of referrals and incidences of filtered emails.
- Ensure that up to date information and relevant links are available on the academy website to encourage parents and carers to engage in learning and self-awareness of safe and potentially unsafe practices when useful technology.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the academy's ESafety policies and guidance.
- Read, understand and adhere to the HACA staff AUP. (ACCEPTABLE USE POLICY)
- Develop and maintain an awareness of current E-Safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed E-Safety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Be aware of what to do if an E-Safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Technical Staff

- Read, understand, contribute to and help promote the Academy's E-Safety policies and guidance.
- Read, understand and adhere to the Academy staff AUP.
- Support the Academy in providing a safe technical infrastructure to support teaching and learning
- Take responsibility for the security of the Academy ICT system.
- Report any E-Safety-related issues that come to your attention to the E-Safety / child protection coordinator.
- Develop and maintain and share an awareness of current E-Safety issues, legislation and guidance relevant to their work.
- Liaise with the local authority, WCAT and others on technical issues.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Regularly review the security of academy information systems and its' users, including up to date virus protection.

Responsibilities of Students

- Read, understand and adhere to the HACA student AUP (Acceptable Use Policy)
- Help and support the academy in creating E-Safety policies and practices and adhere to any policies and practices the academy creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in HACA and at home.

Take responsibility for learning about and adhering to safe practises when using internet based technologies to publish information, including the use of technology for communication and social media.

- Take responsibility for their own and each other's safe and responsible use of technology in HACA and at home, including judging the risks posed by the personal technology owned and used by students inside and outside of HACA
- Respect the feelings, rights, values and intellectual property of others in their use of technology in HACA and at home, including the use of technology for communication and social media.
- Learn about the need to protect personal information, data and media when using technology and the potential consequences of not doing so.
- Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in HACA and at home, or if they know of someone who this is happening to.
- Discuss E-Safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support HACA in promoting E-Safety.
- Read, understand and promote the HACA pupil AUP with your children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that their children use in HACA and at home, including the safe and responsible use of technology for communication and social media.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Encourage and teach their children to respect the feelings, rights, values and intellectual property of others in their use of technology in HACAand at home, including the use of technology for communication and social media.
- 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.
- Model safe and responsible behaviours in your own use of technology.
- Consult with HACA if you have any concerns about their children's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the academy's E-Safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by students.
- Develop an overview of how the Academy ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the academy encourages students to adopt safe and responsible behaviours in their use of technology in and out of HACA
- Support the work of the New Technologies group in promoting and ensuring safe and responsible use of technology in and out of HACA, including encouraging parents to become engaged in E-Safety training and activities via the academy website.
- Ensure appropriate funding and resources are available for the academy to implement their E-Safety strategy.

4) Teaching and Learning

The key to developing safe and responsible behaviours online, not only for students but everyone within HACA community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in HACA but outside as well, and we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings.

- HACA will provide a series of specific E-Safety-related lessons in specific year groups as part of the ICT curriculum, PSCHE curriculum and other lessons.
- HACA will celebrate and promote E-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- HACA will discuss, remind or raise relevant E-Safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, the need to consider the consequences their actions may have on others and/or themselves, the need to check the accuracy and validity of information they use, and the need to respect intellectual property and acknowledge ownership of digital materials.
- HACA will remind students about their responsibilities through an end-user AUP which every student will sign and which will be displayed throughout the school and in HACA planners.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

5) How parents and carers will be involved

It is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this HACA will:

- Include useful links and advice on E-Safety regularly in newsletters and on our academy website
- Include a section on E-Safety in HACA staff handbook to ensure all staff are aware of any changes and amendments to the e safety policy and procedures

6) Managing ICT Systems and Access

- The academy is responsible for ensuring that access to the ICT systems are as safe and secure as is reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The academy will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All users (including staff, pupils and visitors to the academy using ICT) will sign an end-user Acceptable Use Policy (AUP) provided by the academy appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the academy ICT systems, and that such activity will be monitored and checked.
- Students will access the Internet using an individual log-on, which they will keep secure. Whether supervised by a member of staff, or working independently, pupils will abide by the academy AUP at all times.

- Portable college IT equipment is encrypted using bitlocker and any portable USB sticks that are used on this equipment are also encrypted.

- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the Academy AUP at all times.
- Any administrator or master passwords for Academy ICT systems should be kept secure and available to at least two members of staff.
- The Academy will take all reasonable precautions to ensure that users do not access inappropriate material. **However it is not possible to guarantee that access to unsuitable material will never occur.**

- The Academy will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimise risk.

IT IS NOT PERMITTED FOR ANY INDIVIDUAL UNDER ANY CIRCUMSTANCES TO RECORD ANY EVENTS/CONVERSATIONS IN ANY OFFICE/BUILDING IN COLLEGE OR ON ANY PART OF CAMPUS. THIS INCLUDES USING MP3 RECORDERS, MOBILE PHONES OR ANY OTHER RECORDING DEVICE. (This does not include a reception meeting room which has been adapted so that conversations can be recorded. Appropriate signage is in place)

7) <u>Filtering Internet access</u>

HACA uses a filtered Internet service. The filtering is provided through YHGfL.

- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Leader of New Technologies and network manager.
- If users discover a website with potentially illegal content, this should be reported immediately to the Leader of New Technologies and network manager. The Academy will report this to appropriate agencies including the filtering provider.
- The academy will regularly review the filtering and other security systems to ensure they meet the needs of all users.
- Internet use may be monitored by the network manager and users who access inappropriate content may have their network access restricted.

8) Learning technologies in HACA

	Students	Staff
Personal mobile phones brought into school	Students allowed at certain Times (before college, break, lunch and after college)	Staff allowed
Mobile phones used in lessons	Students not allowed except when the teacher has identified that use of these enhances the teaching and learning that is taking place.	Staff not allowed except when it been has identified that use of these enhances the teaching and learning that is taking place.
Mobile phones used outside of lessons	Students allowed at certain Times (before college, break, lunch and after college)	Staff allowed
Taking photographs or videos on personal equipment or playing music without headsets	Students not allowed	Staff not allowed
Taking photographs or videos on school devices	Students allowed with permission	Staff allowed with permission
Use of hand-held devices such MP3 players or personal gaming consoles or tablets.	Students not allowed except when the teacher has identified that use of these enhances the teaching and learning that is taking place.	Staff allowed at certain times
Use of personal email addresses in school	Students not allowed	Staff allowed at certain times with certain providers.
Use of school email address for personal correspondence	Students allowed	Staff allowed
Use of online chat rooms	Students not allowed	Staff not allowed
Use of instant messaging services	Students not allowed	Staff allowed
Use of blogs, wikis, podcasts or social networking sites	Students allowed with permission	Staff allowed with permission
Use of video conferencing or other online video meetings	Students allowed with supervision	Allowed for selected staff

NB Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure that it is age appropriate.

Using email

- Staff and students must use approved e-mail accounts allocated to them by HACA and be aware that their use of the HACA e-mail system will be monitored and checked.
- Students will be allocated an individual e-mail account for their use in HACA
- Students will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Communication between staff and students or members of the wider HACA community must be professional.
- Any inappropriate use of the HACA e-mail system, or the receipt of any inappropriate messages by a user, should be reported to the Leader of New Technologies.

Using images, video and sound

- Pupils will be reminded of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at HACA and at home.
- Digital images, video and sound will only be created using equipment provided by the academy
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

Using blogs, wikis, podcasts, social networking sites

HACA use blogs/wikis/podcasts/social networking/other ways to publish content online to enhance the curriculum by providing teaching and learning activities that allow students to publish their own content. However, we will ensure that staff and students take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by pupils will take place within the academy learning platform / YHGfL blog. Students will not be allowed to post or create content on sites where members of the public have access unless this has been be approved by the Principal before publishing.
- Any public blogs run by staff on behalf of the academy will be hosted on the learning platform and postings should be approved by the Principal before publishing.
- Students model safe and responsible behaviour in their creation and publishing of online content within the academy learning platform. For example, students are reminded not to reveal personal information which may allow someone to identify and locate them. Students will not use their real name when creating such resources. They will be encouraged to create an appropriate ‘nickname’.
- Staff and students are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of HACA

Using video conferencing and other online video meetings

HACA uses video conferencing to enhance the curriculum by providing learning and teaching activities that allow students to link up with people in other locations and see and hear each other. However, we will ensure that staff and students take part in these opportunities in a safe and responsible manner.

- All video conferencing activity is supervised by a suitable member of staff.
- Students do not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
- Video conferencing equipment is switched off and secured when not in use. Online meeting rooms are closed and logged off when not in use.

- Students are be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off academy premises without the permission of the Principal.
- Parental permission will be sought before taking part in video conferences.
- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the academy

Using mobile phones/mp3 players

- Mobile phones/mp3 players may be brought to HACA but should not be used during lesson time allowed except when the teacher has identified that use of these enhances the teaching and learning that is taking place otherwise should be must off at these times. Use of mobile devices in lessons must be via the academy network to ensure safe internet access.

- Student's using mobile phones/mp3 players or other portable devices in and/or between lessons must use them in accordance to the academy policy. If a pupil breaches the academy policy they will have them confiscated and made available for collection at the end of the academy day. Further sanctions will follow for repeat offenders.
- Any contact between parents and students must only be carried out via Reception
- **The academy is not responsible for any lost or stolen phones or music players**.
- Students will be provided with academy mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up such that only those features required for the activity will be enabled.
- Students will be instructed in the safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the academy in a professional capacity.
- Where staff members are required to use a mobile phone for academy duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a HACA mobile phone should be provided and used. 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.
- Staff should be mindful of safe and responsible use of personal devices. Use of any such device in teaching periods should be only for educational activity that has been agreed by SLT.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

Using new technologies

- As HACA we will keep abreast of new technologies and consider both the benefits for teaching and learning and also the risks from an E-Safety point of view.
- The academy will regularly amend the E-Safety policy to reflect any new technology that we use or to reflect the use of new technology by pupils which may cause an E-Safety risk.

9) <u>Protecting personal data</u>

- HACA will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the academy premises without permission of the Principal and without ensuring such data is kept secure.
- HACA portable ICT equipment such as laptops will be encrypted and use of any portable storage device with these machines will also be encrypted using bitlocker.

10) The academy website and other online content

- The academy website does not include the personal details, including individual e-mail addresses or full names, of staff or students.
- A generic contact e-mail address will be used for all enquiries received through the academy website.
- All content included on the academy website will be approved by the Principal before publication.
- The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
- Staff and students must not post HACA -related content on any external website without seeking permission first.

11) Dealing with E-Safety incidents

Regardless of having the best E-safety policies and practice in place, there may still be occasions when E-safety incidents occur. The incidents may be of varying degrees of concern and as HACA we will investigate any incidents individually.
Complaints about Internet misuse will be dealt with under HACA complaints procedure.

Incidents may involve:

- Accidental or deliberate access to inappropriate material
- Inappropriate use of email or other technologies such as mobile phones
- Illegal use of email and other technologies
- Deliberate misuse of the network
- Cyberbullying. This can be defined as 'The use of ICT particularly mobile phones and the internet to deliberately hurt or upset someone'. This includes the use of social media and email. Cyberbullying of any member of HACA community will not be tolerated.

This list is however far from exhaustive. The range of sanctions may include:

- Verbal warning from classroom teacher
- Referral to Head of Year/Division Head
- Suspension of ICT account and/or internet access with parental contact.
- Parental contact
- PIP
- FT exclusion
- Referral to Child Protection Officer
- Referral to Police
- Any complaint about staff misuse will be referred to the Principal
- All e–Safety complaints and incidents will be recorded by the academy, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the academy to resolve issues.
- All members of the HACA community will need to be aware of the importance of confidentiality and the need to follow the official academy procedures for reporting concerns.
- The academy will liaise with local organisations to establish a common approach to

e–Safety.

- The academy will be sensitive to Internet-related issues experienced by pupils out of HACA e.g. social networking sites, and offer appropriate advice.
- The academy will provide appropriate levels of supervision for students who use the internet and technology whilst on the academy site.
- The academy will provide an AUP for any guest who needs to access the academy computer system or internet on site.

Staff Internet Code of Practice (Acceptable Use Policy)

Staff Internet Access

- All staff will have access to Internet resources and e-mail through the academy networks.
- Staff will be assigned a HACA user account and e-mail address. The HACA e-mail accounts are to be used for official correspondence only. Staff must respect each other's privacy with regard to e-mail as they would any other form of correspondence. When using e-mail to communicate with/asses/advice students, professional standards must be upheld.
- Staff will need to be aware that email and internet access is monitored.

Unacceptable Uses

The following uses are considered unacceptable:-

- **Illegal Activities** – Staff will not attempt to gain unauthorised access to any computer system through, or go beyond the HACA's authorised access account. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purpose of 'browsing.'

- **Inappropriate Activities** –

- **System Security** – If in any doubt, staff must seek advice when downloading programmes or files from the ICT Co-Ordinator or network manager.

- **Inappropriate Language** – Restrictions against inappropriate language apply to public messages and material posted on Web pages. When acting in an official capacity on behalf of the academy or using the HACA e-mail accounts, the following points are noted:-
  1) Staff must not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.
  2) Staff must not post information that could cause damage or a danger of disruption.
  3) Staff must not engage in personal attacks, including prejudicial or discriminatory attacks.
  4) Staff must not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
  5) Staff must not knowingly or recklessly post false or defamatory information about a person or organisation.

- **Respect for Privacy** – Staff must not repost a message that was sent privately without permission of the person who sent it. Staff must not post private information about another person.

- **Plagiarism and Copyright Infringement** – Staff must be aware of copyright laws with regard to information on the 'World Wide Web.' If in doubt contact the webmaster of the site from which the information is sought.

- **Inappropriate Access to Material** – HACA computers must not be used to access material that is profane of obscene, that advocates illegal acts or that advocates violence or discrimination towards other people. A special exception may be made for 'hate' literature if the purpose is to conduct research. Staff must not use academy information and communication system in a way that contravenes the LA Code of Practice (Annex A – which has been adopted), or in a way that contravenes the Professional Standards for Teachers.

Due Process

Hemsworth Arts & Community Academy will co-operate fully with Local or Government officials, WCAT officials in any investigation related to any illegal activities conducted through the college.

IT IS NOT PERMITTED UNDER ANY CIRCUMSTANCES TO RECORD ANY EVENTS/CONVERSATIONS IN ANY OFFICE/BUILDING IN HACA OR ON ANY PART OF CAMPUS. THIS INCLUDES USING MP3 RECORDERS, MOBILE PHOTES OR ANY OTHER RECORDING DEVICE.

Wakefield Local Authority Equipment Policy – Annex A

This document explains the Council's policy on the use of electronic equipment.

This is a policy for the proper use of the Council's electronic equipment and breach of the policy may lead to disciplinary action being taken against you, up to and including dismissal. Electronic equipment includes computers, telephones, fax machines and other mobile devices including hand held recording devices.

Electronic equipment provided by the Council if for the use of employees at work or undertaking Council work and for people not directly employed by the Council but authorised to use it.

The internet is one of the many ways in which we communicate and gather information. Inappropriate or excessive use of the internet is no different from inappropriate use of any other form of communication or media while at work. Any mis-use (online or off-line) when you should be working could lead to disciplinary action.

The council encourages you to use electronic equipment at work for personal training and development. This should be approved by your manager and comply with the standards expected and restriction on use as set out in this policy document. Personal use of any equipment in works time (and in your own time if it incurs costs) should always be agreed with your manager along with a system of repaying any costs incurred. These may be accumulated for periodic or annual payment to reduce administration costs.

If you need any information that may relate to colleagues or relatives, always check with your manager first to ensure it is appropriate.

The Councils electronica and communications systems automatically log an individuals' use of its equipment when it's connected to its systems. Such logs are in the form of traffic data. For example telephone calls are listed on itemised bills.

You must not use any of the Council's electronic facilities to:-

- Knowingly send, receive, access, download or post any inappropriate material (including to newsgroups and other internet based forums). This means material which is illegal, obscene, indecent, abusive, racist, sexist, libellous, in beach of copyright, defamatory or otherwise inappropriate.

- Send anonymous messages, engage in gossip, or make libellous statements about individuals or organisations.

- Make statements which appear to represent the Council when they are personal views.

- Make derogatory or malicious remarks or express derogatory opinions about the Council.

- Knowingly infringe copyright or intellectual property rights or send or receive anything illegal or fraudulent.

- Pursue personal business interests, engage in gambling or for political purposes not directly linked to your job.

- Disclose or allow anyone else to use your user name and password to gain unauthorised access to any of the Council's systems.

- Knowingly engage in any activity that threatens the integrity or availability of the Council's systems.

- Try to breach the Council's security systems (hack) in any area, whether inside or outside the Council.

- Use automated Internet based information services that 'push' information to the desktop (Internet Channels or news 'ticker tape' services), except for legitimate business use.

- Transmit, receive, copy or store digital media (including software, music, video etc) except for legitimate purposes which comply with the copyright and licensing regulations.

- Use message attachments to transmit, download or store inappropriate material and media.

- RECORD ANY EVENTS/CONVERSATIONS IN ANY OFFICE/BUILDING IN COLLEGE OR ON ANY PART OF COLLEGE CAMPUS. THIS INCLUDES USING MP3 RECORDERS, MOBILE PHOTES OR ANY OTHER RECORDING DEVICES.

You must seek your manager's approval prior to engaging in these activities:-

- Personal use of any equipment or facilities during working hours.

- Use of instant messaging services.

- Visits to website in the course of your work which may be perceived as being inappropriate.

- If you need any information that may relate to colleague's or relatives.

Legitimate use of electronic and communications equipment:-

- Internet, computers, mobile phones and other electronic equipment are provided for work should take precedence at all times over personal use.

- Some personal use is allowed but in your own time – before or after work or unpaid lunch breaks. Personal use is still subject to restrictions.