Electronic Communications Policy

Introduction

This policy addresses the use of electronic communications by staff and will apply to all Academy employees provided with authorised access to the Academy's equipment, systems or information. A student-friendly version of this will be produced for Academy students and will be covered as part of the ICT curriculum.

It is every staff member's responsibility to read and comply with the requirements of the policy and its appendices. It is also the responsibility of every employee to report any breaches of this code e.g. misuse of e-mail, Internet, Intranet, telephones etc. either to their line manager, the Principal or the Chair of Governors.

Every staff member has a duty of care for equipment such as phones and computers that are provided for their use. It is expected that staff will take reasonable steps to maintain the security and safety of equipment. This includes not leaving equipment in view in unattended vehicles or classrooms and storing it securely when not in use. If you use a PIN to access your SIM, do not leave the PIN number in the same place as your SIM card. Repairs to equipment must only be carried out by authorised personnel, therefore any equipment failure or problems must be reported to the ICT department.

Misuse or loss of communications equipment due to negligence will result in staff being requested to reimburse costs to the Academy and may result in disciplinary action.

Whilst using the Academy's communications technology systems staff should also ensure they comply with the associated Academy policies on Data Protection and Information Security.

Failure to follow this code may constitute a serious disciplinary offence, which could lead to dismissal. It could also lead to criminal or civil action if illegal material is involved or if legislation, such as the Data Protection and Computer Misuse Acts, is contravened.

Registered Office: King's Leadership Academy, Hillock Lane, Woolston, Warrington WA1 4PF
Telephone: 01925 817939. www.greatschoolstrust.org

Electronic Communications and Law

The most relevant legislation regulating electronic communications are:

- The Data Protection Act 1998 (Relating to the use of personal information)
- The Computer Misuse Act 1990 (Relating to unauthorised access and creation or distribution of computer viruses)
- The Copyright Designs and Patents Act 1988 (which relates to unauthorised copying often referred to as software piracy)

Breach of any of the above can constitute a criminal offence. Where the Academy believes a criminal offence has taken place, it has a duty to inform the Police. Using the Academy's facilities in any way to break the law will be considered as gross misconduct under the Academy's Disciplinary Procedure.

Content and Usage

Material accessed via the Internet or sent by E-mail is subject to some automatic filtering. The Internet filtering process aims to ensure that the majority of material which is offensive, unsuitable or illegal cannot be accessed.

- You should be confident that anything which you access or send meets the following criteria:
  - There is a legitimate business need (other than permitted personal use described later)
  - That it is within the law and does not breach copyright
  - That you have the authority to send the message (i.e. when committing the Academy to a course of action)
  - Communications must comply with the Academy's Policy on Bullying and Harassment.

There have been a number of disciplinary cases in other institutions nationally relating to the sending and receiving of unsuitable messages. (See Appendix 1 for the type and content of material considered inappropriate). Be aware that the use of the Academy's facilities for the sending or receiving of such messages is strictly prohibited; if you receive a message that breaches this policy please refer to the guidance in the introduction.

- General advice on e-mail etiquette can be found in Appendix 3.

Issue of Mobile Phones and other handheld technology

The criteria for the issue of mobile phones and other handheld technology will meet one or more of the following criteria:

- The issue of equipment will significantly reduce risk such that employees can be reached in the case of emergency.
- A measurable business benefit with regards to cost savings is gained through the issue of mobile phones and/or other devices
- There is a clear benefit resulting in enhanced working through better access.
- Sufficient legitimate out of hours contact is required to maintain cover and/or emergency contact for the service.

Personal Use

Reasonable use of the Academy's Electronic Communications systems is permitted providing that:

- It does not interfere with work performance or divert employees from their duties
- It is not used for furthering outside business interests or for personal monetary gain
- The use of the Internet conforms to all other requirements in this policy
- Usage does not adversely affect the performance of the e-mail system or Academy network.

The only personal usage tolerated is in the following areas:

Email

- A minimal level of mundane personal use is tolerated. This use must be outside your working time. Be aware that emails may be monitored and that personally sensitive information should not be sent. Messages should not contain anything that others may find offensive or distasteful. Examples of material that is not permitted are those with a sexual content, jokes or chain letters, a more comprehensive list is in Appendix 1. Personal encryption of messages is prohibited.

If you receive messages which breach this policy then you should do the following:

- If you know the sender, reply advising them that Academy Policy prohibits that type of message and ask them not send any more similar messages.

- If the message is from another Academy employee then contact your Line Manager for further advice.
- If you are offended or upset by the message you should refer to the Bullying and Harassment Policy, discuss it with your Line Manager or the Principal or Vice Principal.
- If the message is from outside the Academy and you do not know the sender then advice the ICT staff who can arrange to have messages from specified senders blocked.

Such material may for example not be identifiable until the e-mail is opened and in these cases staff will not be held responsible provided that they report it immediately. These items should never be passed on to other Academy or non-Academy individuals.

Telephones/Faxes

- Personal use of landlines should not be excessive and any private calls should be avoided in normal working hours unless deemed 'essential'. You will be expected to reimburse the Academy for the cost of these calls in accordance with the Academy protocol.

Internet Access

- Limited personal use is tolerated outside of working time. Although every attempt is made to prevent access to unsuitable sites it is your responsibility not to access any sites containing unsuitable material (some examples are listed in Appendix 2). Be aware that all Internet access is routinely monitored and logged and sites containing unsuitable material are prohibited at all times. The downloading of information for personal use is not permitted at any time.
- All Internet connections should be via the King's Leadership Academy system. Under no circumstances should there be a dial-up connection through any other Internet service provider (ISP) such as BT, AOL etc.

Unacceptable Use

- The accessing or distribution of offensive, illegal or unsuitable material is unacceptable and subject to disciplinary action and/or prosecution.

Offensive material is anything which is abusive, intimidating, malicious or insulting. The persistent abuse of power, or the belittling of someone, either in public or private, which makes them feel upset, threatened, humiliated, vulnerable or undermines their self-confidence, through the use of Information Technology is unacceptable and will be deemed to be bullying or harassment. The Academy's staff policies will give a list of examples of what constitutes bullying and harassment. In the specific context of electronic communications please see Appendix 1 for examples.

Employees must not engage in:

- Posting information that may tend to disparage, threaten, or harass others on the basis of gender, race, age, disability, religion or belief, sexual orientation or national origin.
- Posting statements that are defamatory or information that is false or misleading concerning the Academy or other organisations and their services/products.
- Distributing confidential or sensitive information about the Academy or its partner organisations that might compromise its confidentiality.
- Deliberately using email in such a way that it constitutes bullying or harassment.
- Originating or participating in email chain letters.
- Substantial personal use of email, including the transmission of large documents or programs which will add an unnecessary burden to the network.
- Sending jokes, games and other non-work related emails, in a "chatty" and informal style could lead to problems for both the Academy and its staff – do not assume others share your sense of humour.
- The email system must not be used to send or receive inappropriate material (either within an e –mail or as an attachment) such as adult material (pornography), racism \ hate, drugs, terrorist and violence, gambling, share dealing, paedophilia etc.
- Sexually explicit material or materials of a disturbing nature must not be received, archived, stored, distributed, edited or recorded using the Academy's network or computing resources (Appendix 1 provides examples of what would be considered inappropriate materials)
- Use of Internet based email accounts i.e. Hotmail is prohibited

The list above gives examples of the types of behaviour which constitute violation of the policy. This is not an exhaustive list and there may be other violations which are not listed here.

Misuse

Where misuse has been identified, members of staff need to be aware that disciplinary action will be taken. The following, although not an exhaustive listing, is an example of actions, which would warrant serious disciplinary action with possible suspension/dismissal and in certain cases potentially criminal prosecution:

- Staff accessing some websites e.g. child pornography and terrorist sites.
- Staff accessing, distributing materials of an unsuitable nature (please refer to Appendix 1 & 2) via e- mail or within an e-mail attachment.
- Defacement of the Academy website and Intranet.

- Any involvement in 'hacking', virus propagation and 'mail bombing' of the Academy or any website or Contravention of the Computer Misuse Act.

Security Arrangements and Controls

Security incidents including the following examples, must be reported to the Academy's ICT Service
Desk immediately:

- Where it is believed another person is using an employee's ID/ password. Attempts to log on as another user will result in cancellation of e-mail and Internet access and may result in disciplinary proceedings. Internet passwords should not be disclosed to anyone else. Each Internet user is totally accountable and responsible for usage on his / her account this also is applicable where users have one "log on" password that gives access to both Internet and e mail.
- If a staff member believes another user is accessing prohibited material.
- Construction of personal / business [non- Academy] websites.
- The settings of the PC anti-virus software being amended or dis-enabled.
- Employees engaging in 'hacking' activities into non- Academy web-sites (serious disciplinary action may result).
- If an employee accidentally accesses a prohibited site – this should be reported to the Line Manager/ICT staff as soon as possible after the incident and details of the incident should be logged.
- Unauthorised devices e.g. IPods, Cameras, Non-Academy Memory Sticks, external hard drives should be checked by ICT staff before being connected to Academy computers as this could pose a risk to the security of the Academy's network.
- Any suspicious e-mails or attachments should not be opened or forwarded to others as they may contain a virus.
- When using telephones, either landlines or mobile handsets and whether for personal calls or in the course of your duties, you should take into consideration the location where you are making the call, whether or not it will distract colleagues and whether or not the nature of the telephone conversation is appropriate in front of colleagues, students and/or visitors to the Academy. It is also important to be courteous and take into consideration that colleagues may not want to be interrupted by your telephone conversations.
- Personal mobile phones should not be used during working hours unless necessary and should be kept on silent/vibrate when in the classroom.

Monitoring

The Academy has developed a range of measures for the use of this technology in order to protect the Academy and its staff from potential litigation or complaint about inappropriate access and use of communications. Such measures already in place include:

- A filtering system which filters e-mails and images/attachments contained within e-mails of an unsuitable, offensive or illegal nature.
- A security system of filtering inappropriate Internet sites to prevent access and record attempts to access prohibited sites which are offensive and illegal.
- General monitoring of the extent of usage of all forms of communications, such as e - mail, internet, telephone and fax usage which is reported to Line Managers/Principal on a regular basis.
- An e-mail disclaimer is automatically included in outgoing e-mails.

Monitoring is undertaken to:

- Provide evidence of Academy transactions
- Inform for training purposes and standards of service
- Access Academy communications e.g. to check e-mail etc. when employees are on holiday or sick
- Prevent or detect unauthorised use of the Academy's communication systems or criminal activities
- Maintain the effective operation of the Academy's communication system including protection against viruses
- Ensure the Academy's policies and procedures are followed.

Routine monitoring of the Academy's communication can and does take place. Do not assume that there will be any degree of privacy for personal messages. Members of staff need to be aware that consent to such monitoring is a pre-requisite of using the Academy's communications technology.

Leaving the Academy

On leaving the Academy you must return all equipment.

Equal Opportunities

In implementing this policy all members of staff must take into account the School's Equal Opportunities policy. Staff must ensure that no person is disadvantaged on the grounds of gender, race, disability, sexual orientation, age, religion or belief.

Monitoring, Evaluation and Review

Great Schools for All Children will review this policy at least every two years and assess its implementation and effectiveness.

Appendix 1 – Offensive and Unsuitable Material

The following identifies the type of content considered inappropriate:

- Aggression including threats or violence, abuse or obscenities
- Material which promotes illegal acts
- Sexual advances, propositions, suggestive remarks
- Sexually explicit or pornographic material
- Discrimination of any kind including insults or "jokes" which are related to a person's sex, sexuality, religion or belief
- Racist abuse including "jokes", insults or taunts
- Offensive abuse, ridicule, "jokes" or name calling relating to a person's disability
- Material which the person knows, or ought to have known, would offend a colleague with particular sensitivities, even if it is not explicitly offensive, e.g. religious views or beliefs, gender identity, sexual orientation etc.
- Care needs to be exercised in the tone, language and content of any messages sent by or to other Academy or external equipment i.e. text messaging

This is not an exhaustive list. There may be other material which is not listed here which is offensive or illegal. In general terms messages should not be sent that are likely to cause offence to other employees or bring the reputation of the Academy into disrepute.

Appendix 2 - Unsuitable Web-Sites

Certain websites cannot be accessed as a filter controls the access to the majority of unsuitable websites; examples of such sites are detailed below along with other examples of unacceptable use:

- Accessing, displaying, downloading or disseminating threatening, obscene or pornographic material including sites that display full or partial nudity in a sexual context or sites that depict or graphically describe sexual acts or activity etc.
- Racism \ Hate.
- Militancy & Extremist.
- Drugs - sites that promote or provide information about the use of prohibited drugs (unless for work related purposes).
- Terrorist/violence/weapons
- Gambling
- Internet auctions
- Games – downloadable entertainment or games, or playing games over the Internet

- Hacking - sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases
- Share dealing
- Paedophilia
- Downloading files, software or videos from the Internet or e-mail system unless there is a business related use for the material i.e. software that may enable a Web page to be viewed correctly
- Downloading, using or distributing copyrighted material without proper authorisation
- Construction of personal / business [non- Academy] websites
- Sending and requesting 'junk mail', fund raising requests or chain letters are banned.
- Saving data to Internet files [known as 'X' files] is not allowed.

Appendix 3 - Policy on the Use of Electronic Communications

Checklist of Do's and Don'ts

Electronic communications have transformed the way we work. They improve efficiency, productivity, and information sharing and customer service. But technology is moving at an increasingly fast pace and revised advice and guidance on the use of electronic communications is necessary.

A detailed document (Electronic Communications Policy) has been produced which brings together all the current advice and guidance under one policy.

This is a checklist of what to do and not to do which should be read in conjunction with the full policy. Usage of electronic communications is monitored and filtered to make sure that the facilities are not misused. Limited personal Internet use is allowed outside normal working hours.

All e-mail messages are recorded and management may, under certain circumstances, monitor specific usage and have access to mailboxes.

Access to web-site material containing adult material, racism / hate, drugs, gambling, terrorist activities, share dealing or paedophilia is banned at all times. Non-business sites such as entertainment, sport and travel should be limited to reasonable access during non-working hours i.e. lunch-time.

Where the Academy believes a criminal offence has taken place, it has a duty to inform the Police. Using the Academy's facilities in any way to break the law will be considered as gross misconduct under the Academy's Disciplinary Procedure.

Fax and Telephone (Landlines & Mobiles)

DO

- Answer telephones promptly and politely (internal & external)
- Take messages accurately
- Limit personal calls for emergencies only (landline)
- Reimburse the Academy for any personal calls made
- Take care when disclosing sensitive or confidential information by telephone
- Switch off mobile phones during lessons, meetings, presentations & when driving
- Restrict the faxing of lengthy documents wherever possible
- Take care over the content, style and tone of faxes
- Include a confidentiality statement on the cover sheet for confidential information to be sent

DON'T

- Make international and premium rate calls unless authorised
- Make excessive private calls during work hours
- Disclose sensitive, confidential information on a fax or over the telephone

Electronic Mail (E-mail)

DO

- Keep messages short, clear and to the point
- Ensure comments are accurate, justified and suitably worded
- Use file compression software for large attachments – and ensure the recipient has the facility to open them
- Arrange for large attachments or graphics to be sent by other means i.e. internal mail
- Check your mail box regularly and clear unwanted e-mails
- Use folders to store items for efficient retrieval
- Do not store messages unnecessarily either in Outlook folders or in personal folders – delete messages 'past their sell by date' regularly
- Be aware that all emails can be monitored

- Ensure the “out of office” facility is enabled for planned absence
- Use the Academy’s recognised email signature format
- Avoid taking paper copies of emails unless for correspondence files or meetings
- Avoid “mail storms” – long discussions sent to a wide distributions list
- Target your message - use distribution lists to send “all staff” emails rather than highlighting individual names
- Beware of viruses
- Remember emails have the same legal status as paper mail

DON’T

- Use all capitals or use gimmicks such as smiley faces or fancy fonts – this is very informal
- Open any suspicious emails or attachments
- Reveal your password to anyone else
- Attempt to log on as another user
- Read or send personal emails in normal working hours
- Make excessive personal use of emails
- Send sensitive or emotional messages
- Send an email if it could embarrass the receiver or the Academy
- Send or request ‘junk mail’, fund raising requests or chain letters
- Reply to SPAM (Slang term for unsolicited mail)
- Send or import software programs by email or any other means unless there is a recognised business need
- Use the urgent flag read receipt too often
- Use inappropriate language or include abusive comments that can be interpreted as threatening harassing or insulting
- Express personal views which may be misinterpreted as those of the Academy
- Distribute or store any material of a sexually explicit image or material of a disturbing nature via email or attached to an email

Internet and Intranet

DO

- Beware of viruses and follow security instruction and anti-virus procedures
- Recognise all internet access can be monitored
- Keep personal use to a reasonable level of access outside normal working hours, over lunch or after work

- Use Academy equipment for researching work projects and keeping up to date on developments
- Talk to your line manager if you are unsure about any issues regarding access
- Use the intranet to access Academy policies and procedures

DON'T

- Access unauthorised web-sites / material
- Use internet based email services e.g. 'Hotmail'
- Download software onto your computer without authorisation
- Disclose your password to anyone else
- Disable or amend the settings of your anti-virus software
- Attempt to 'hack' into any web-sites or computer systems
- Construct non Academy web-sites
- Participate in non-professional chat services
- Attempt to connect to the internet through any non-Academy dial-up connection i.e. BT / AOL
- Place documents on the intranet without prior authorisation
- Illegally copy any computer software
- Play games on the Internet
- Introduce knowingly viruses to the Academy network Induce or allow others to do any of these things