

The Littlehampton Academy



Email, Internet and ICT Policy

Introduction

The Academy believes that the effective use of information and communication technologies can bring great benefits and will work to develop them into the work and learning of all staff and students. The Academy recognises the e-safety issues and this policy will ensure appropriate, effective and safe use of electronic communications.

Purpose and objectives

- To encourage students and staff to make good use of the significant and growing educational opportunities presented by access to the internet and the use of e-mail and other electronic communication.
- To enable the Principal to do what is reasonable in all the circumstances to safeguard and promote the welfare of students and to minimise the risk of harm to the assets and reputation of the Academy.
- To prevent abuse of e-mail and internet facilities available at the Academy.

Email Risks

The power of instantaneous, worldwide communication by email potentially poses significant risks to the Academy and members of the Academy community in relation to:

- Defamation or malicious falsehood, through the careless or vindictive composing, sending and/or distributing of gossip or messages maligning a person, a group of persons or an organisation (including the Academy).
- Unlawful harassment and/or discrimination on the grounds of sex, race or disability between one member of staff and another, for which the Academy may be vicariously liable.
- 'Electronic bullying' between staff and/or students for which the Academy may be vicariously liable.
- The ease with which email can be used for non-educational, social or personal matters, thereby wasting time, slowing down transmissions for other users, and incurring costs for the Academy.
- Users forgetting or not realising that email messages can be retrieved even once deleted and may have to be disclosed in the event of subsequent litigation.
- The possibility that an unauthorised contract may be formed by a student or member of staff having ostensible authority on behalf of the Academy.
- Interception, unintended receipt or unauthorised reading of emails by others, for example through hacking, disclosure of passwords or careless use of distribution and address lists.
- Plagiarism and/or breach of copyright by sending, receiving or using, without appropriate permission and acknowledgement, the intellectual property belonging to another.
- Revealing personal information about oneself or another (in breach of the Data Protection Act 1998).
- Transmission of viruses as e-mail attachments.

Internet Risks

In addition to the features and dangers of simple email, the internet facilitates and provides other forms of electronic communication and information such as access to and use of websites,

newsgroups, list servers, links, games and programmes. There is also the growing commercial use of the internet to sell goods and services worldwide.

- Some of the images and text available on the internet to view, download or attach to an e-mail are or may be harmful to students, staff and the Academy community as a whole eg pornographic, racist, sexist, blasphemous or violent material.
- A further danger is that of importing viruses onto the Academy's network, or passing viruses to a third party, via material downloaded from or received via the internet or brought into Academy on storage devices such as USB sticks.
- Some files may be very sizeable and therefore costly, and time consuming, to download. Large files also take up valuable memory capacity, thus having an adverse effect upon the performance of the Academy's computer system.

Email Protocols

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is not allowed.
- Never open attachments to emails unless they come from someone you already know and trust. They could contain viruses or other programs which could destroy all the information and software on your computer.
- The sending and receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. Always report such messages to a member of staff.

Internet Protocols

- Do not access the internet unless for study or for school authorised/supervised activities.
- Do not use the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials that are unlawful, obscene or abusive.
- Respect the work and ownership rights of people outside the school as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' facilities over the internet. This takes up valuable resources which could be used by others to benefit their studies.
- The Academy will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Never arrange to meet anyone unless your parent/carer or teacher goes with you. People you contact online may not always be who they seem.
- Do not give out personal details (telephone number, address) to others. Remember that people may want your personal information in order to impersonate or contact you in ways that may harm you.

Video-conferencing Protocols

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students' age.

Security and Privacy Protocols

- Do not disclose your password to others, or use passwords intended for use by others.
- Never tell anyone you meet on the internet your home address, your telephone number, the Academy's name, or send them your picture unless you are given permission to do so.
- Do not use the computers in a way that harasses, harms, offends or insults others.

- Respect and do not attempt to bypass security in place on the computers, or attempt to alter the settings.

Equipment Protocols

- Do not install, attempt to install or store programs of any type on the computers/laptops without permission.
- Do not damage, disable, or otherwise harm the operation of computers/laptops, or intentionally waste resources.
- Do not use the computers/laptops for commercial purposes e.g. selling or buying goods.
- Do not open files brought in on removal media (e.g. USB memory/flash drives, cd's, etc.) until they have been checked with anti-virus software and been found to be clear of viruses.
- Do not connect mobile equipment to the network (e.g. laptops, tablet PC's, PDA's etc.) until they have been checked with antivirus software and been found to be clear of viruses.
- Do not eat or drink near computer equipment.
- The Academy reserves the right to charge users either wholly or in part for the replacement cost of any equipment or resources that are damaged through failure to follow this policy.

Sanctions

- Where a student breaches the Academy's Email and Internet Protocol, the Governors have authorised the Principal to apply any sanction which is appropriate and proportionate to the breach including, in the gravest circumstances, exclusion.
- Where a member of staff breaches the Protocol, the Governors have authorised the Principal to apply the Academy's Disciplinary Procedure which may, in appropriate circumstances, lead to dismissal.
- Where a member of staff wishes to complain about email or internet use, the Governors have authorised the Principal to make use of the staff grievance procedure.

Procedures

This Policy authorises the Principal to implement and enforce procedures dealing with the following:

- Entering into and maintaining a filtered service with the Academy's internet service provider.
- The purchase and upgrading of appropriate software and support, including in relation to virus detection.
- Setting up and maintenance of autosignatures for outgoing emails.
- Training students and staff in using email and the internet, particularly in the light of this Policy.
- Control of physical access to the Academy's computers.
- Supervision and appropriate monitoring of students' use of email and access to the internet.

The Liability of the Academy

- Unless negligent under the terms of this Policy, the Academy accepts no responsibility to the student or parents or staff caused by or arising out of a student's or member of staff's use of email and the internet whilst at Academy.
- The Academy does not undertake to provide continuous internet access. Email and website address/es at the Academy may change from time to time.