

# Light Hall School e-Safety Policy

## Students

Access to the school network is provided for you to carry out recognised schoolwork and extra-curricular activities, but only on the condition that you agree to follow the schools e-safety policy.

### General

- All files held on the network will be treated as school property, including e-mail. ICT Network staff may look at files and communications to ensure that the system is being used responsibly. You should not expect that your work and e-mails will always be private. You should also be aware that the network manager can access your computer area at any time from anywhere on the school network without you knowing about it.
- You are responsible for all use of your account on the school network. Never tell your password to anyone else or let them use your account. If you think someone has discovered your password or is using your account, tell a member of the staff immediately. Never use another person's account. Try and avoid using predictable passwords eg., birthdays, etc.
- You must not install any programs on a school computer or run them from a local source, except with the permission of a member of the staff.
- You must not attempt to by-pass any security systems, modify any profile or install registry entries.
- You must only use a printer for school-related work and activities. Careless or deliberate wasting of paper will result in your printing facility being withdrawn.
- Eating and drinking are strictly prohibited in any ICT room.
- Always make sure that you have completely logged off the computer before leaving it unattended.
- No computer equipment (except laptops) may ever be removed from its location or tampered with. Any such interference with school property is a most serious offence.
- 'Hacking' i.e. unauthorised access or use of personal information is a serious criminal offence. Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files may be considered a criminal offence under the Computer Misuse Act 1990.
- That the unauthorised copying of software is not permitted.
- Installation copying or transmitting obscene material may be considered a criminal offence. In addition, any material in your account which the school considers inappropriate or offensive will be removed immediately, and other sanctions will follow.

### The Internet and E-mail

- The filtered Internet service is provided for you by Solihull Education Authority to conduct genuine research and communicate with others. All the sites you visit are recorded. Remember that access is a privilege, not a right and that access requires responsibility at all times.
- *You will be taught what internet use is acceptable and what is not and will be given clear objectives for Internet use*
- You must never send, display, access or try to access any obscene or offensive material.
- You must not use obscene or offensive language in e-mails. Remember that you are a representative of Light Hall School on a global public system - never swear, use vulgarities, or any other inappropriate language. Remember that the school has the right to read your e-mails.
- You must never harass, insult or attack others through electronic media. Within Light Hall School this is bullying and will be punished as such. Remember that any e-mail you send can be traced. A recipient of an offensive e-mail from you may take legal action against you.
- Never copy and make use of any material without giving credit to the author. Not only are you infringing copyright, but also you will be guilty of plagiarism.
- Never reveal any personal information, the home address or personal phone numbers of yourself or other people.
- Check with a member of Staff before opening unidentified e-mail attachments or completing questionnaires or subscription forms.
- *The School will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.*
- *Never reveal any personal information, the home address or personal phone numbers of yourself or other people*
- *If you discover unsuitable sites, the URL (address), time date and content must be reported to Solihull ICT Services, and where appropriate the school e-Safety officer.*
- *Social networking sites and newsgroups will be blocked unless a specific use is approved.*
- *You must never give out personal details of any kind which may identify you or your location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, specific interests and clubs ect.*
- *The school will work in partnership with Solihull MBC and Becta to ensure filtering systems are as effective as possible.*

- *You may only use approved email accounts on the school system.*
- *You must immediately tell a teacher if they receive offensive email.*
- *You must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.*
- *Use of words included in the filtering/checking "banned" list will be detected and logged.*

### **Games**

- Games may never be played from your account, from another source, or over the Internet. Never attempt to download any games or executable programs from the Internet without the express permission of a member of staff.

### **Video Conferencing**

- *All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.*
- *IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the internet.*
- *Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323ID name*
- *External IP addresses should not be made available to other sites. Video conferencing contact information should not be put on the school website*
- *You should ask permission from the supervising teacher before making or answering a videoconference call.*
- *Video conferencing should be supervised appropriately for the pupils age.*
- *When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.*
- *Recorded material should be stored securely.*
- *If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners Intellectual Property Rights (IPR).*

### **Sanctions**

- Any infringement of the Code of Conduct will be reported to the Head of ICT and the Network Manager. Punishments will vary dependant on the severity of the infringement.
- For more serious offences, such as the transmission of offensive material or 'hacking', the Headteacher, and your parents will be informed. Note that if a criminal offence appears to have been committed, the school will refer the matter to the police.