



LYNDON SCHOOL HUMANITIES COLLEGE

E-SAFETY AND ICT ACCEPTABLE USE POLICY

E-safety encompasses internet technologies and electronic communications. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Lyndon School Humanities College has considerable computerised information technology resources available for staff and students and this will continue to grow and develop. These systems are increasingly critical to the day to day function and management of the school as well as teaching and learning.

It is vital that the users, staff and students are protected from any potential harm that may result from unacceptable and inappropriate use.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, and Data Protection.

All staff and students are responsible for e-safety at Lyndon School. E-safety will be regularly reviewed and monitored by the ICT Strategy Group; reporting to the Leadership Team and Governors.

E-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure service from Solihull MBC
- National Education Network standards and specifications.

Further Information

Becta e-safety

www.becta.org.uk/schools/esafety

Teaching and learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The school Internet access will be designed expressly for students use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear guidance for Internet use.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Students will be taught how to evaluate Internet content

- Schools must ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students must be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly (at least annually) by the ICT Strategy Group.
- Virus protection will be installed and updated regularly by both Solihull Council and Lyndon School Humanities College.
- The school will install specialist software for the management of e-safety. All students and staff will be made aware of this software in the relevant internet access agreement.
- Security strategies will be discussed with the Local Authority as appropriate.
- E-safety rules will be posted in all networked rooms.
- Staff and students will be informed that network and Internet use will be monitored.

E-mail – (students)

- Students must only use approved e-mail accounts on the school system.
- Students must immediately tell a member of staff if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters (or e-mail) is not permitted.
- Staff should only use e-mail for specific and relevant job related communications.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone and fax numbers. Staff or students personal information will not be published.
- The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Social networking and personal publishing

- School will endeavour to block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Managing filtering

- The school will work in partnership with Solihull Council, DCSF and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the Network Manager.
- The filtering methods will be reviewed regularly (at least annually) by the ICT Strategy Group.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time, unless specifically instructed by a member of staff as part of the teaching and learning. The sending of abusive or inappropriate text messages is forbidden.

Authorising Internet access

- The school will maintain a current record of all staff and students who are granted access to school ICT systems.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SMBC can accept liability for the material accessed, or any consequences of Internet access.
- The school will provide appropriate training and CPD for the ICT technical team and other staff as appropriate.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by an Assistant Head Teacher.
- Any complaint about staff misuse must be referred to the Head Teacher (or in her absence the Deputy Head) or Chairman of Governors.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the Internet

- Only those who are students at Lyndon or are employed by Lyndon School Humanities College will be given access to the Internet.

Enlisting parents' and carers' support

- Parents' attention will be drawn to the School's e-safety Policy in newsletters, the school brochure and on the school website.

Staff e-safety

- Staff must be aware of the following :
 - Solihull MBC ICT Security, A Guide for Employees
 - Solihull MBC Communications Policy and Guidanceboth are available on Solnet, or via the ICT Technicians.
- Staff must be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential and expected.
- Staff must use the internet facilities, including e-mail, sensibly, professionally, lawfully. Use should be consistent with their professional duties and with respect for colleagues.
- Staff must **not** use the school's systems to access material from the internet which is inappropriate to their role, may cause offence or upset to others, is illegal, or which could jeopardise the security of the school systems. Examples include:
 - downloading of pornographic material
 - playing online games or using "chat rooms"
 - surfing websites for personal reasons
 - personal internet shopping
 - personal messages and communications which are not relevant to their professional role

Staff are advised to take care when accessing "chat rooms" or posting personal information on the Internet both, within and outside school. They must be aware that this information is available world wide and may place them in a position which could compromise their own professional role and that of their colleagues.

Staff should never use their own personal email address to contact students.