SOUTH LEICESTERSHIRE COLLEGE

# E-Safety Guidelines and Procedures (SS011)

## 1. Background

South Leicestershire College recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of the potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the college while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read alongside other relevant college policies e.g. safeguarding.

## 2. Purpose

The purpose of this document is to guide staff and learners to the safe use of college IT systems and Internet both at college and off site.

## 3. Definition: What is an e-Safety Policy?

E-Safety guidance helps to promote the use of technology to enhance learning within the college and will ensure students get the most from it, by encouraging responsible online behaviour. E-safety guidance helps minimise risk and embed important principles such as

- keeping personal information private
- considering the implications of any content posted online
- not uploading or posting inappropriate, offensive or illegal content to own or other online spaces.

## 4. Scope

This guidance applies to all learners, staff or others who have access to the college IT systems, both on the premises and remotely. Any user of the colleges' IT systems must adhere to all relevant policies. The guidance applies to all use of the internet and electronic communication devices such as e-mail, mobile devices, social networking sites, and any other systems that use the internet for connection and providing of information.

## 5. Responsibilities

- The College has a responsibility to ensure college resources are used responsibly and safely by learners and staff.
- All managers are responsible for ensuring that their staff are aware of this policy and procedure and how it operates.
- Individual members of staff have a responsibility to: Be aware of this policy and procedure and how it operates.
- Individual learners have a responsibility to use college resources and the Internet in a responsible and safe manner and in the event of any e-Safety concerns to contact a member of the Safeguarding Team, their tutor or the IT Department.

## 6. Technologies

The technologies and services covered by this policy include computer, internet, electronic communication and mobile devices such as mobile/smart phones and PDAs.

- Websites
- Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video and Music downloading

Students may be working online in college, at home or elsewhere. They may be using personal devices not covered by college security systems and everyone to needs to understand the risks and act accordingly.

## 7. Stakeholders

This means that designing and implementing e-safety guidance demands the involvement of a wide range of interest groups:

- Principal
- Governors
- Senior Managers
- Teachers and Support Staff
- All students, particularly young people and vulnerable adults

This guidance should be read in conjunction with the college's Safeguarding Policy, Harassment and Bullying Policy and Disciplinary Policy. It will be reviewed annually by the college.

## 8. Creating a Safe ICT Learning Environment

The college has implemented systems to minimise the risk of accessing inappropriate and unacceptable information, applications, websites etc. These are:

- Firewalls to stop unwanted intrusion from external locations and to ensure that students/staff cannot access external websites without using the Internet content filtering system
- Internet content filtering to categorise web site content and by the use of rules either allow/disallow access to websites
- Virus protection to check all files, emails and websites for viruses and clean/quarantine the virus as appropriate
- Network security to limit access, through the use of usernames and passwords, to students and staff's own files or designated shared access areas
- User Access Control to restrict the ability of students and staff to install software and make changes to the computer systems.

## 9. Monitoring

The E- Services team monitors access to all college computer systems. This includes the logging on/off computers systems, Internet activity, Virtual Learning Environment (Moodle), and e-mails. Monitoring will only be used to confirm or investigate compliance with college policies and procedures.

## 10. Internet Use

It is impossible to be completely protected while using the internet, but simple steps to reduce the risks may be taken, as outlined below.

## 11. Search Engines Sites

Search engines enable the rapid search of the internet for information, whether this information is text, image or sound. Searching consists of entering a word or words into a search box and clicking the search button, which sets in motion a search engine that automatically produces a list of the addresses of websites relevant to the words entered. Many search providers also offer the facility for the user to search for images, video and audio content.

The more accurate the search is (i.e. using more than one relevant word), the more relevant the search results will be and the less likely that unwanted results will be prominently returned. For example, if searching for information on the planet Mercury, entering 'planet mercury' into the search box will get more relevant results than just entering 'Mercury'.

Take care to spell correctly when typing in a search. Even a small typing error can bring up unwanted results.

Remember that not all the information in websites returned in searches is reliable. There are steps that may be taken to assess the quality of the information found (see www.quick.org.uk).

There are two types of search results (see above for more information on this):

- Automated search results
- Sponsored listings

Search providers usually separate and label these but it is important to be aware of the difference and be able to differentiate the the results of the search provider used.

Whichever search provider is chosen, it is important to become familiar with the provider's service, especially its safety advice, its filter, how to contact the search provider, and how sponsored listings are differentiated from other search results.

## 12. Social Networking Sites

Social networking sites, like Facebook, Twitter or Bebo are online 'communities' of internet users with similar interests. Members of the community create an online 'profile' which provides other users with varying amounts of personal information.

Once users have joined the network, they can communicate with each other and share things like music, photos and films. The sites are a fun way to stay connected with friends, family and peers.

As with most potential online dangers, the problems can start if you do not look after personal information properly. The risks you need to be aware of are:

- Cyber bullying (bullying using digital technology)
- Invasion of privacy
- Identity theft
- Seeing offensive images and messages
- The presence of strangers who may be there to 'groom' other members.

## 13. Staying safe using social networking websites:

- Don't publish personal information like location, email address, phone number or date of birth
- Be very careful about what images and messages are posted, even among trusted friends. Once they are online they can be shared widely and are extremely difficult to get removed
- Keep a record of anything abusive or offensive received and report any trouble to the site management. Most sites have a simple reporting procedure, normally activated by clicking on a link on the page.
- Be aware that publishing or sharing anything which would mean breaking a copyright agreement is illegal.

- If you make an online friend and want to meet up with them in real life, ensure you have a responsible adult with you to check the person is who they say they are.
- Be aware of online scams. Offers which seem too good to be true usually are.
- Do not to get into any online discussions about sex as this tends to attract potentially dangerous users.

## 14. E-mail

- Do not forward chain letters to anyone else, just delete them.
- Do not impersonate anyone else using e-mail.
- Do not use e-mail to send comments or information that is defamatory or libellous, or use e-mail as a means of harassment, intimidation, annoyance or bullying to anyone else. The sender of an e-mail should only send messages the contents of which they would be happy to receive or have read out in court. E-mail messages are admissible as evidence.
- Do not reply to pestering, offensive or suggestive e-mails. Students should report such occurrences to a member of the Safeguarding Team, tutor or IT Department
- The biggest cause of computer viruses is sent by email, often innocently. If you think you have received a virus or are suspicious about an email received, delete the email without opening it and report it to the IT Department.

## 15 e-Safety Concerns and Complaints

All queries and concerns should be addressed to a member of Safeguarding Team or a tutor in the first instance. Proven incidents of internet misuse or other breaches in acceptable use will be taken very seriously and may be dealt with through college procedures relating to conduct, harassment or bullying.

Concerns relating to safeguarding, including child protection must be referred immediately to the Safeguarding Team.

**Acknowledgements** Some information in this document was taken from www.direct.gov.uk and is subject to Crown copyright.