e-Safety Policy

2023-2024

Date Approved	March 2023
Approved By	Finance and Strategy Committee
Review date	March 2026
Responsibility	Director of IT and Network Services

E-safety policy

A. Introduction.

Sandwell College Group seeks to promote and facilitate the proper and extensive use of Information and Learning Technologies in the interests of teaching and learning. However, the College recognises thatthe ever changing nature, coupled with the accessibility, openness and power of these technologies can provide a potential risk to the College community. This e-safety policy aims to minimise the levelsof risk associated with a wider use of ILT, but it would be unwise to think that this policy can potentially remove the risk factors. This e-safety policy aims to provide systems, techniques and training so members of the College can recognise the risks and manage their own e-safety. It is closely linked with the College Safeguarding network for the times when additional support may be needed.

B. Definitions.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate our learners about the benefits, risks and responsibilities of using information and learning technology. It provides safeguards and raises awareness to enable users to control their online experiences. E-safety is a child safety/learner safety issue rather than an ICT one, so is an extension of general safeguarding within the College.

C. Purpose and Scope.

This policy defines how Sandwell College intends to promote e-safety and provide safeguarding measures for its community. It seeks to define methods of fulfilling the College's obligations to:

1. Safeguard and promote welfare
2. Uphold and enforce the Prevent Duty and promotion of British Values.
3. Provide sufficient security (data encryption, access, anti-virus)
4. Remove and/or block unlawful or unsuitable material
5. Report crime
6. Maintain an incident response procedure
7. Deter discrimination and harassment
8. Promote positive attitudes
9. Challenge prejudice
10. British Values.

This policy applies to all members of the College community who have access to and are users of College ILT systems, both in college and remotely.

This policy links with the following policies:

Acceptable Use Policy: IT and ILT Equipment and Resources

JANET Acceptable Use Policy

Combined Higher Education Software Team (CHEST) Code of Conduct

Any other user terms and conditions which are part of an on-line database to which the College subscribes or has use (FENC, NLN, Shibboleth etc.)

Sandwell College Safeguarding Policy

Sandwell College Policy on Harassment and Bullying of Learners

All Equality and Diversity Policies

D. Roles and Responsibilities.

It is the responsibility of the Governors, through the Executive and Senior Management Teams and College managers, to ensure the effectiveness of and compliance with this policy. It is the responsibility of **all members of the College** and visitors to the College to adhere to its provisions and to contribute towards a safe environment for all.

The responsibility for the supervision of this e-safety policy and to ensuring effective responses to incidents is delegated jointly to the Student Services Manager – Designated Safeguarding and Prevent Lead or the Executive Director of Finance and Resources in order to ensure that both safeguarding and ILT issues are addressed in any incident.

Responsibility of individuals for reporting incidents.

All members of the College community, including visitors, are required to report any incidents or concerns regarding inappropriate content and material, even if accessed accidently. If the individual is unsure whether the incident is in relation to e-safety, then they should still report the issue to the Head of Centre, a designated Safeguarding Officer or the Director of IT and Network Services who will make the relevant judgement.

Students can report any incidents to their lecturers, members of the ILT support or Student Services teams, or any other member of College staff.

Staff can report incidents to any senior staff, or to members of the ILT support or Student Services teams. Safeguarding concerns can also be reported via the CPOMS portal.

All staff must be aware that any incidents disclosed to them should be dealt with sensitively and with a degree of confidentiality, as outlined in the Safeguarding training and policy.

Information about **ALL reported incidents** must be forwarded to the Safeguarding and Prevent Lead, who will determine the seriousness of the incident and take the necessary actions.

F. The Issues.

The use of new technologies can put young people and vulnerable adults at risk within and outside the College. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The risk of exposure to radicalisation, potential to use the Internet to search for or share extremist messages or social profiles
- The sharing / distribution of personal images without an individual's consent or knowledge, including sexting.
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other policies (eg behaviour, anti-bullying and safeguarding policies).

G. The College's Obligations:

1. Safeguard and promote welfare.

The College has an existing robust and effective policy for safeguarding and promoting welfare which is available on the Virtual Learning Environment. The policy is supported by a Safeguarding team who as part of their role will support e-safety. The College also has a Safeguarding Board and e-safety is a key part of the action plans for this group.

The College also has anti bullying polices and equality policies which support the welfare of learners.

2. Prevent.

Sandwell College has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "Prevent". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

Members of the College community must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. Systems are in place to detect certain terms, and their repetition via the filtering system. These are reported to theto the Safeguarding team.

Social networking is restricted on college systems in order to reduce distraction and the risk of radicalisation via these networks.Staff in Learning Centres have access to the Smart Synchroneyes system which in intended to support learners, but can also be used to manage usage and ensure correct use of the systems available. Users who attempt to bypass College security (e.g. by using Tor Browsers, ultrasurf plug in) are subject to College Disciplinary procedures.

3. Provide sufficient security (data encryption, access, anti virus).

Access to the College network is via individual log in for both students and staff. Students have access to secure storage on their 'H' drive. The College uses firewalls as part of its security measures and all incoming e-mails are scanned. Antivirus software is available on all PCs and laptops and is updated regularly.

Student and staff individual log ins enable the College to track Internet sites used by that log in. This process would be carried out by the Network team at the request of the nominated safeguarding managers.

All users should be aware of the IT Security Policy and should not risk any personally identifiable data by the use of portable media/devices. Users can seek guidance on this from the ILT support team. The current advice is that this data should only be available via a secure log in through the College systems.

4. Remove and/or block unlawful or unsuitable material.

The internet is filtered for undesirable sites and there is a procedure for blocking any sites which may be missed by the filtering system, or where a corporate decision has been taken to block certain sites which are causing issues with course management, or distress to learners. (social networking, for example).This simple procedure is to phone or e-mail the ILT Helpdesk with details of the problem site.

Monitoring software is used in IT classrooms and Learning Centres and bases. This contributes towards the safe use of the PCs for all.

The filtering software provides reporting of search terms which have been identified as being potential risk topics. The report enables the identification of individuals who are searching for subjects/terms identified as risk areas and so supports the Prevent strategy of the College.

5. Report crime.

The importance of e-safety means that any breach in law should be reported appropriately and promptly.

Computers suspected of being used for illegal or inappropriate purposes should be isolated and the Director of IT and Network Services should be contacted to arrange the removal of the PC in order to carry out necessary investigations.The person code of the user should also be identified so network usage can be assessed.

If the material is illegal, the police should be contacted by the Director of IT and Network Services or Head of Centre

6. Maintain an incident response procedure: Misuse.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that appropriate procedures are used to investigate, preserve evidence and protect those carrying out the investigation. As above, the Director of IT and Network Services should be contacted and the computer isolated from use.

Incidents involving learners should be addressed using the College disciplinary procedure, which includes a role for an investigating officer. Similarly, any incidents involving staff should be addressed through the HR Department.

All e-safety incidents should be logged centrally by Safeguarding and Prevent Lead. The statistics from these logs will be reviewed and monitored by the Safeguarding Steering Group.

Maintain an incident response procedure: Incidents off College premises.

Incidents which originate off College premises can affect the conduct and abilities of learners on premises (e.g cyber- bullying which may originate with a contact who is not a College member). These incidents should be dealt with and reported in the same way as an incident which has occurred within the College community and the learner will have access to the College support network.

7. Eliminate discrimination and harassment, Promoting positive attitudes and challenging prejudice. British Values

The College has an Equality and Diversity policy which is monitored by the Learners Quality and Curriculum Committee and the Equality sub groups. Issues of harassment and bullying are encompassed in a relevant policy and any issues of e-bullying and e-harassment will be dealt with using this policy and the College disciplinary procedures.

The college also has a Fundamental British values policy which sets out the framework in which Sandwell College will ensure that it actively promotes the Department of Education's five part definition of British values.

Students receive tutorials and opportunities within their induction and tutorials. Topics relevant to esafety which embed British Values include:

- Safeguarding and Prevent
- Staying Safe
- Online Safety
- Legal rights and responsibilities

H. Curriculum Use of the Internet – e-safety.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. The College uses web filtering software to try and block inappropriate content. However, no system can be one hundred percent reliable. Therefore, if users come across any inappropriate content/websites, they must report it to their lecturers or the ILT support team, who will review the content and arrange for it to be blocked. The web filtering software reports will be regularly reviewed, and the system tested, by the Network Services team.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit. The College uses monitoring software and training is available for lecturers on how to use the software.
- Sometimes, for good educational reasons, students may need to research topics which result in internet searches being blocked. In such a situation, staff can request, via the ILT Helpdesk (e-mail, phone, in person) that the Network team can temporarily remove that site from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

I. Use of digital images.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, users need to be aware of the risks associated with sharing images and with posting digital images on the internet or sending images via multimedia messaging. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The College will include information about these risks in the sessions described in section K below.

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet eg on social networking sites from home.

Members of the College must not use mobile phones to carry out recordings, but should use standalone cameras (bookable via the ILT Helpdesk) and so avoid the increased risk of images being inadvertently transferred from mobile phones to the Internet

J. Data Protection.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data only when absolutely necessary and using encryption and secure password protected devices.

Removal of content on third party sites over which the College has no control:

- If the content is illegal or considered to cause serious harm and distress, then the police will be contacted and informed.

- If the content has no serious implications, however an individual wants the content removed, then the ILT support team will try and advise the individual how to go about this. However, it is not the responsibility of the College to organise the removal of such content.

K. Education and Awareness:

e-safety will be promoted across the College to staff and students via posters, leaflets and an area on Virtual College

1. Staff.

The ILT staff induction includes e-safety and refers to this policy and the Acceptable Use of IT/ILT Policy. ILT staff and Network Services staff are happy to discuss e-safety issues and concerns about their own e-safety as well as those of their learners.

- The VLE has an e-safety area which can be directly accessed from the useful resources area on the Student portal.
- Stay safe on-line leaflets are available in the Learning Centres.
- E-safety posters are on display around the College.

2. Learners.

The induction process for students will include the issues of e-safety, how learners can protect themselves and what they need to do if they feel their e-safety is compromised. The induction is reinforced by information available on the Student Virtual College.

- The Safeguarding policy requires that safeguarding and safety tutorials are designed and delivered for learners.
- The Student Survey asks whether students feel safe.
- Internet safety is incorporated into the ILT induction.
- The VLE has an e-safety area which can be directly accessed from the useful resources area on the Student portal.
- Stay safe on-line leaflets are available in the Learning Centres.
- E-safety posters are on display around the College.

L. Work experience/Work based Learning.

Formal checks of workplaces are carried out by the Occupational, Health and Security Unit and a Letter of Understanding is issued to participating employers/work experience providers. The workplace check and the Letter both take child protection into account and so include safeguarding and e-safety considerations.

The reporting system for issues of e-safety will follow the established procedures for safeguarding, but assessors need to include e-safety in their workplace visits and report any concerns.

M. Privacy.

Privacy of PCs and laptops connected to the network cannot be guaranteed as the network is monitored. In addition, monitoring software provides an ability to monitor activity in IT classrooms and Learning Centres/Bases. If a member of staff discovers a cause for concern when using monitoring with a group, they should report it to the Safeguarding team.

N. Use of personal technology devices on College premises.

The College supports the use of user's own devices. Specific use of BYOD is covered in detail in the Acceptable Use of IT and ILT Policy.

Users have the ability to log in to the Eduroam network using current College credentials. This also provides some network security for users.

O. Reviewing the Policy.

This e-safety policy will be subject to an annual review. This is necessary owing to the constant emergence of new technologies and the consequent requirement to mange the associated risks. Responsibility for initiating the review lies with the Director of IT and Network Services

P. Further Guidance, Support and Contacts.

The main contacts who can provide technology expertise in relation to e-safety are:

- Director of Funding, Examinations and Information Services
- Director of IT and Network Services
- Head of Safeguarding

The up-to-date contact details for the above can be obtained from College reception/switchboard/VLE phone book.

For further clarification and advice on this policy, please contact the above.

Appendix

Simplified code of use

The following is a very brief summary of the main points of the Acceptable Use of ILT and IT Policy. Adherence to the Code will support e-safety.

- **Governance**

  Don't break the law, do abide by the College's regulations and policies, and do observe the regulations ofany third parties whose facilities you access.

- **Identity**

  Don't allow anyone else to use your IT credentials, don't disguise your online identity and don't attempt to obtain or use anyone else's.

- **Infrastructure**

  Don't put the institution's IT facilities at risk by introducing malware, interfering with hardware or loading unauthorised software.

- **Information**

  Safeguard personal data, respect other people's information and don't abuse copyright material. Remember that mobile devices may not be a secure way to handle information.

- **Behaviour**

  Don't waste IT resources, interfere with others' legitimate use or behave towards others in a way that would not be acceptable in the physical world.