LONDON BROOKES
C O L L E G E

# E-SAFETY POLICY AND PROCEDURES

## London Brookes College

**Rationale**

**The purpose of this policy is to:**

- set out the key principles expected of all members of the college community at LBC with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of LBC
- assist college staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other college policies.
- ensure that all members of the college community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

**The main areas of risk for our college community can be summarised as follows:**

**Content**

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

**Contact**

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

**Conduct**

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)

copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

**Scope**

This policy applies to all members of LBC community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of college / academy ICT systems, both in and out of LBC premises.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the *college* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the college, but is linked to membership of the college. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by other policies related to behaviour.

The *college* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of college.

| Role | Key Responsibilities |
|---|---|
| Vice-Principal(s) | • To take overall responsibility for e-safety provision<br>• To take overall responsibility for data and data security<br>• To ensure the college uses an approved, filtered Internet Service, which complies with current statutory requirements<br>• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant<br>• To be aware of procedures to be followed in the event of a serious e-safety incident.<br>• To receive regular monitoring reports from the E-Safety Co-ordinator / Officer<br>• To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures( e.g. network manager) |
| E-Safety Co-ordinator / Designated Child Protection Lead | • takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the college e-safety policies / documents<br>• promotes an awareness and commitment to e-safeguarding throughout the college community<br>• ensures that e-safety education is embedded across the curriculum<br>• liaises with college ICT technical staff<br>• To communicate regularly with SMT to discuss current issues, review incident logs and filtering / change control logs<br>• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident<br>• To ensure that an e-safety incident log is kept up to date<br>• facilitates training and advice for all staff<br>• liaises with the Local Authority and relevant agencies<br>• Is regularly updated in e-safety issues and legislation, and be aware of the |

| Role | Key Responsibilities |
|---|---|
| | potential for serious child protection issues to arise from:<br>• sharing of personal data<br>• access to illegal / inappropriate materials<br>• inappropriate on-line contact with adults / strangers<br>• potential or actual incidents of grooming<br>• cyber-bullying and use of social media |
| Governors | • To ensure that the college follows all current e-safety advice to keep the children and staff safe<br>• To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.<br>• To support the college in encouraging parents and the wider community to become engaged in e-safety activities |
| Network Manager/technician | • To report any e-safety related issues that arises, to the e-safety coordinator.<br>• To ensure that users may only access the college's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed<br>• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)<br>• To ensure the security of the college ICT system<br>• To ensure that access controls / encryption exist to protect personal and sensitive information held on college-owned devices<br>• the college's policy on web filtering is applied and updated on a regular basis<br>• that he / she keeps up to date with the college's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant<br>• that the use of the *network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction*<br>• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.<br>• To keep up-to-date documentation of the college's e-security and technical procedures |
| Teachers | • To embed e-safety issues in all aspects of the curriculum and other college activities<br>• To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended college activities if relevant)<br>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws |

| Role | Key Responsibilities |
|---|---|
| All staff | • To read, understand and help promote the college's e-safety policies and guidance<br>• To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current college policies with regard to these devices<br>• To report any suspected misuse or problem to the e-safety coordinator<br>• To maintain an awareness of current e-safety issues and guidance e.g. through CPD<br>• To model safe, responsible and professional behaviours in their own use of technology<br>• To ensure that any digital communications with pupils should be on a professional level and only through college based systems, never through personal mechanisms, e.g. email, text, mobile phones etc. |
| Pupils | • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations<br>• to understand the importance of reporting abuse, misuse or access to inappropriate materials<br>• to know what action to take if they or someone they know feels worried or vulnerable when using online technology.<br>• to know and understand college policy on the use of mobile phones, digital cameras and hand held devices.<br>• To know and understand college policy on the taking / use of images and on cyber-bullying.<br>• To understand the importance of adopting good e-safety practice when using digital technologies out of college and realise that the college's E-Safety Policy covers their actions out of college, if related to their membership of the college<br>• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in college and at home<br>• to help the college in the creation/ review of e-safety policies |

**Communication:**
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the college website / staffroom
- Policy to be part of college induction pack for new staff
- Policy to be discussed with pupils at the start of each year.

**Handling complaints:**

- The college will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a college computer or mobile device. Neither the college nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by tutor / Head of Year / E-Safety Coordinator / Headteacher;

- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to LA / Police.

- Our E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with college / LA child protection procedures.

**Review and Monitoring**

The e-safety policy is referenced from within other college policies:

- The college has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the college
- The e-safety policy is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SMT and approved by Directors and other stakeholders. All amendments to the college e-safeguarding policy will be discussed in detail with all members of teaching staff.

**Checked on 4th August 2021 by Cillian Logue**