

LONDON BROOKES COLLEGE Policy on IT Security

1.1 Definitions

For the purposes of this policy:

- “User” is anyone who uses LONDON BROOKES COLLEGE hardware or software;
- “LONDON BROOKES COLLEGE” shall be taken to mean hardware, software or any other IT related system operated by LONDON BROOKES COLLEGE;
- “Inappropriate use” shall be interpreted by the Vice Principal to include accessing pornographic images, the unlicensed and illegal use of software and the unauthorised uploading of software onto LONDON BROOKES COLLEGE. Such misuse will be subject to LONDON BROOKES COLLEGE disciplinary procedures;
- “Confidentiality” means ensuring that information is accessible only to those authorised to have access;
- “Integrity” means safeguarding the accuracy and completeness of information and processing methods;
- “Availability” means ensuring that authorised users have access to information and associated assets when required.

2.0 Related Documents

Data Protection policy

2 Rationale

LONDON BROOKES COLLEGE needs to ensure that its IT systems are secure from interruption and interference to protect its business interests and fulfil its requirements while ensuring that information is treated correctly with regard to the sometimes conflicting interests of confidentiality, integrity and availability.

3 Core Principles

- LONDON BROOKES COLLEGE must enable confidence in and compliance with third party partner organisations who are subject to EU/UK legislation in this regard.
- Security of the LONDON BROOKES COLLEGE system will be proactively monitored and breaches of security
- will be reported, investigated and the cause corrected as soon as possible.
- Only appropriate use will be made of LONDON BROOKES COLLEGE equipment
- LONDON BROOKES COLLEGE retains its right to monitor the use of its systems by any user in order to protect its legitimate business and reputational interests.
- Appropriate external systems will be employed by LONDON BROOKES COLLEGE to help ensure the security of its systems

4 Implementation

The Vice Principal has overall responsibility for ICT within LONDON BROOKES COLLEGE but can delegate responsibility for IT Security a reputable third party specialist consultant and/or organisation. Vice Principal will;

- report to the Principal and advise regarding the development and on-going effectiveness of this policy;
- ensure that appropriate controls for initial user set up and password access are in place with the requirement that there is a periodic change to passwords.
- ensure that this policy is updated at least every third year, or when regulations applying to
- IT security are issued or changed;
- ensure that, as regards internet use, LONDON BROOKES COLLEGE will comply with those of the internet connection that LONDON BROOKES COLLEGE subscribes to.;
- Ensure that appropriate systems are in place to protect LONDON BROOKES COLLEGE from infection by a
- Virus and similar cyber-attack;
- Ensure that staff are appropriately inducted in the secure and efficient use of information and operate systems to minimise any loss or breach;
- ensure that the LONDON BROOKES COLLEGE website is compliant;
- Ensure that breaches of security are reported and acted upon in a timely way.
- Ensure that, should a breach of security occur, appropriate remedies are identified and in
- place to recover any lost data and rectify the cause.

5 Quality Assurance

LONDON BROOKES COLLEGE reviews IT security as part of its three year cycle of reports.

The SMT will from time to time examine the arrangements in place to ensure that the risk of LONDON BROOKES COLLEGE failing to comply with this policy is minimised.

Curriculum and support teams

Each Tutor shall be responsible for ensuring that IT security arrangements under her/his control comply with this policy.

Checked 4th August 2021 by Cillian Logue