Christ the Redeemer College
London

Christ the Redeemer College - Acceptable Use of IT Policy

Scope

CRC provides access to computing and IT resources for staff and students for both work and study purposes. Staff and students have access to computing and IT resources, to the internet and World Wide Web. This use can also be extended to visiting lecturers and other staff on request, who must also adhere to this policy.

This Acceptable Use of IT Policy covers the security and use of all the information and IT equipment owned and provided by Christ the Redeemer College (CRC). It also includes the use of email, internet, voice and mobile IT equipment and non-college equipment used on the premises and connected to the college internet system e.g. personal laptops and tablets. This policy applies to all CRC's employees, students and visitors who have been given access to the college IT system.

This policy applies to all information, in whatever form, relating to CRC's business activities worldwide, and to all information handled by CRC relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by CRC or on its behalf.

Computer Access Control – Individual's Responsibility

Access to CRC's IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the CRC's IT systems.

All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Allow anyone else to use their user ID and password on CRC's IT system.
- Leave their user accounts logged in at an unattended and unlocked computers.
- Use someone else's user ID and password to access CRC's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to CRC's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Connect any non-CRC authorised device to the CRC network or IT systems.
- Store CRC data on any non-authorised CRC equipment.
- Give or transfer CRC data or software to any person or organisation outside CRC without the authority of CRC.
- Use the college IT facilities to draw people into acts of terrorism and/or extremism or promote terrorism/extremism.
- Enable unauthorised 3rd party access to the IT system.

Individuals may:

- Attach headphones to College computers.
- Attach memory drives to college computers.

Individuals must:

- Log out of their account if leaving the computer for an extended period of time.

Internet and Email Conditions of Use

- Use of CRC's internet and email is intended for business and study use.
- Personal use is permitted where this does not affect the individual's business or study performance, is not detrimental to CRC in any way, not in breach of any term and condition of employment and does not place the individual or CRC in breach of statutory or other legal obligations.
- Use of the college internet and email to draw other people into acts of terrorism and/or extremism or promote terrorism/extremism is strictly forbidden.

Monitoring

CRC may monitor any aspect of its IT systems which are available for staff and students and may record any communications.

CRC may log and retain records of all electronic communications including email exchanges and web browsing between users of the IT facilities and any external organisation for one year.

Disciplinary Action

Any incident which is considered to be in breach of this policy may lead to disciplinary action.