CEQ STAFF IT POLICY

This Policy applies to all CEQ staff

(this policy is to be read in conjunction with CEQs Data Protection Policy)

Confidentiality and Data Protection

1. Information deemed confidential by CEQ, and which may also be confidential according to GDPR includes: -
    a. Employee records
    b. Information concerning the banking or finances of CEQ
    c. Data of members/suppliers/partners
    d. Any other documentation marked as confidential
2. IT users have a responsibility to immediately report the theft, loss or unauthorised disclosure of any information that is accessible or stored on any electronic or computing device (including laptops or phones) belonging to CEQ
3. IT users must ensure that any electronic devices that they use to access any information belonging to CEQ, including in particular confidential information, have suitable up to date anti-virus and anti-malware software.
4. All IT users must ensure that any confidential information is protected in accordance with relevant data protection laws (further information can be found in the CEQ Data Protection Policy).
5. For network maintenance and security purposes, authorised individuals may monitor systems, equipment and network traffic at any time.
6. IT users must ensure that all files, emails and records that they work on during the course of their employment are backed up on a regular basis (preferably daily) on an automated backup system if possible.
7. Any use of a new private cloud provider or new cloud storage supplier agreement/contract must be authorised in advance by the CEQ Trustees' Governance & Compliance Committee to ensure the necessary compliance checks are undertaken prior to any appointment.
8. IT users must not:
    a. Use confidential information for their personal benefit or profit.
    b. Disclose confidential information to anyone outside of CEQ.
    c. Replicate confidential documents and files and store them on insecure devices.
9. Breach of this policy is likely to lead to disciplinary action even in the case of unintentional breach or disregard of this policy, depending on its frequency and seriousness.

Security for Devices

10. IT users are expected to -
    a. Ensure that all devices they use to access information (including confidential information) belonging to CEQ have up to date anti-virus and anti-malware software.

b. Make sure that they have a secure password for all records, sites and services that they use for on behalf of CEQ and that these passwords are kept securely and accessible by their line managers in case of emergency.

c. Understand the privacy and security settings on any computers or phones used to access information belonging to CEQ.

d. Ensure that if they access information belonging to CEQ (whether confidential or not) from a personal device, that they do so via a separate user account that no one else e.g. family members can access.

e. Make sure their computers and phone log out automatically after 15 minutes and requires a password to log back in

Laptops and Mobile Phones

11. Any laptops, mobile phones and other devices that are supplied to you by CEQ for the better performance of your role and which are portable remain the property of CEQ, and must be returned to your line manager, a Trustee of CEQ or a Member of CEQ to be nominated by your line manager or a Trustee of CEQ-

    a. Upon request from your line manager or a Trustee of CEQ or

    b. Upon the termination of your employment.

Acceptable Use Policy

12. Any electronic devices, including computers and mobile phones that are the property of CEQ may not be used directly or indirectly by an IT User for the download, creation, manipulation, transmission or storage of:

    a. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

    b. unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;

    c. unsolicited “nuisance” emails;

    d. material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;

    e. material which advocates or promotes any unlawful act;

    f. material that brings CEQ into disrepute.

    g. Breach of this policy is likely to lead to disciplinary action even in the case of unintentional breach or disregard of this policy, depending on its frequency and seriousness.

CEQ Employment Committee: 26 May 2021

CEQ Trustees' Governance & Compliance Committee: 27 May 2021

Approved by Trustees June 2021. Revision due 2024