Data security policy

1. Purpose

The purpose of this policy is to ensure that data and information held by CUREE is securely stored and transferred, and that staff are aware of how they should carry this out. CUREE abides by relevant legislation related to, but not limited to, the Data Protection Act (2018)[1], and the General Data Protection Regulation (GDPR) but this policy and the procedures underpinning it is designed to conform to the higher standards of data security demanded by Government departments and other official agencies.

2. Scope

This policy applies to all CUREE staff, sub-contractors and consultants and to all data and information held by CUREE.

3. Accountability

CUREE has board-level accountability for data security issues, with the Managing Director assuming senior responsibility for the area, and who is CUREE's Data Protection Officer.

4. Human resources

4.1. Responsibility

All CUREE staff and contractors are responsible for conforming to this policy as directed by the Managing Director.

4.2. Corporate awareness

Staff contracts of employment include provision related to their compliance with this policy and any associated procedures. Staff are offered advice on data security from the Data Protection Officer and given training on the practical implications of data security. CUREE has produced a short guide on data security for staff, supplemented with periodic updates, bulletins and alerts around particular issues (e.g., ransomware) which are available via the intranet.

4.3. Security checks

Security background checks are carried out for all employees conducting primary research. All employees are required to provide proof of the following before commencing employment:

- Nationality and immigration status
- Identity
- Full and permanent address
- Employment history

- Unspent criminal records

Staff likely to be visiting education establishments are also checked by the Disclosure and Barring Service (DBS).

4.4. Third party contracts

CUREE's contracts with sub-contractors include a clause requiring compliance with Data Security Policy, in order to enforce compliance with our data security requirements.

4.5. Registration with the ICO

CUREE holds registered entry on the Information Commissioner's Office (ICO) database, detailing the personal data we hold and process.

5. IT infrastructure

5.1. System security

CUREE has implemented Cloud solutions to application and data storage and management based primarily on the Office 365 suite of products with One Drive and SharePoint being the principal storage platforms. These incorporate high levels of access security, data security and data backup/resilience. Some use is also made of Google Workspace primarily to maintain noncritical public data access and Google Sites facilities. A single RAID 5 Network attached storage device is used for working file access and backup. Access to this is password protected. The device itself runs several security routines, and checks and warns of security weaknesses.

5.2. System access

CUREE operates in a distributed network environment with staff and associates working from home (and elsewhere). All CUREE IT resources are password protected and most now require two-factor authentication. Only staff members with valid passwords can access the resources, and staff are required to ensure that any sensitive folders are password protected. Home workers can obtain remote access to our systems via regular cloud access which extends all standard security processes to their local devices. Google Device Management is enforced on all mobile devices accessing the CUREE data systems (requiring, for instance, strong passwords on devices and providing for administrator remote data wiping).

6. Data transfer

6.1. Data encryption

CUREE enforces the encryption of all sensitive data prior to transfer through compression and encryption tools (e.g. Axcrypt). Staff should ensure the encryption of data designated as sensitive before transfer, and should seek assistance from the SOM. This policy applies to data transferred by email or removable devices (e.g. flash drives or Universal Serial Bus devices).

6.2. Secure storage

All hard copies of data are appropriately secured and protected in a locked environment.

6.3. Secure disposal

CUREE enforces a secure disposal policy for all electronic media, portable or otherwise. All unwanted portable devices or hardware content should be returned to the IT team, who will arrange for disposal using secure erasing technology. Paper copies of sensitive data and information are shredded with a strip-cut shredder.

6.4. Incident management

CUREE has a disaster management policy (separately documented). If sensitive data is mislaid, lost or stolen, staff should notify the Data Protection Officer, who will decide on an appropriate action following CUREE's formal GDPR data breach protocol - which may include informing clients of a data breach and reporting it to the ICO.

7. Structured risk assessments

7.1. Documented assessments

CUREE enforces the documented assessment of data security risks in projects. All project management documents (PMDs) must include a section evaluating data security risks, and ways to respond to these. Project highlight reports monitor data security risks and how these are handled. These documents are scrutinised at 6-weekly progress meetings.

7.2. Technical assessments

CUREE carries out regular testing of its network and physical security through regular penetration testing.

8. Personal Data

8.1. Personal data

- Personal data may only be used in accordance with instructions from the individual concerned and only to the extent as is necessary for the provision of services for the client or as is required by Law or any Regulatory Body.
- Files containing personal data will be password protected and access only permitted to staff directly involved in the project.
- Personal data should only be collected if it is specifically required by a particular project or service. For example, while names and email addresses may be required for the distribution of a survey, they should not be included in any documents used during the analysis of the data.

- Where personal data is included on hard copy the header should include the words "Personal Data – Protect" on each page.
- Prior written consent from clients is required if data is to be transferred to any subcontractors.

8.2. CUREE personnel

Data about CUREE personnel will be subject to the protocols outlined for the treatment of personal data as outlined above. However, it is not practical to extract the identification data elements (name, address etc) from the rest of the record.

8.3. Requests for personal data or complaints relating to the client's obligations

In the event of a request from a Data Subject for access to their Personal Data, CUREE will notify the client of the request, where the data is held for the purposes of a specific project, within 5 working days. In the event of a complaints or requests relating to the client's obligations under the Data Protection Act, CUREE will notify the client within 5 days, providing full details and any other information requested by the client, in so far as it does not breach the Data Security Act.

8.4. Processing data outside of the EEA

CUREE will not process personal data from outside the European Economic Area (EEA) without the prior written consent of the client. We have confirmed that our Cloud storage providers hold our data on equipment sited within the EEA and can certify their own compliance with the DPA 2018 or the GDPR as relevant.

9. Indemnity

9.1. Professional Indemnity

CUREE holds Professional Indemnity cover at a value of £1,000,000.

[1] Information Commission (ICO) *Data Protection Act*
Accessed at: https://ico.org.uk/for-organisations/data-protection-act-2018/