1. Introduction

1.1 AECC University College collects, holds, processes, and shares personal data and this needs to be suitably protected. The University College manages all data according to the General Data Protection Regulation and the Data Protection Act.

1.2 Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

1.3 Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs and the University College take every step to avoid such incidents.

2. Purpose and Scope

2.1. The University College is legally obliged to implement an institutional framework to oversee the security of all personal data during its lifecycle, including delegating clear lines of responsibility for the management and security of all personal data shared within the organisation.

2.2 This policy sets out the procedures to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the University College.

2.3 This policy relates to all personal and special categories (sensitive) data held by the University College regardless of format.

2.4 This policy applies to all staff, students and patients at the University College. This includes temporary, casual or agency staff and contractors, consultants and suppliers and working for, or on behalf of the University College.

2.5 The objective of this policy is to prevent, contain and to minimise the risk associated with any potential breach and consider what action is necessary to secure personal data Where a breach has been identified the AECC University College will take all appropriate action to prevent any such event occurring in the future.

3. Definitions of breach/incident

3.1 For the purpose of this policy, data security breaches include both confirmed and suspected incidents ‘near misses’.

3.2 An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems, or personal

data, either accidentally or deliberately, and has caused or has the potential to cause damage to the University College's information assets and / or reputation.

3.3 An incident may include but is not restricted to, the following:

3.3.1 Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);

3.3.2 Equipment theft or failure;

3.3.3 System failure;

3.3.4 Unauthorised use of, access to or modification of data or information systems;

3.3.5 Attempts (failed or successful) to gain unauthorised access to information or IT system(s);

3.3.6 Unauthorised disclosure of sensitive / confidential data;

3.3.7 Website defacement;

3.3.8 Hacking attack;

3.3.9 Unforeseen circumstances such as a fire or flood;

3.3.10 Human error;

3.3.11 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

4. Reporting a breach

4.1 Any individual who accesses, uses or manages the University College's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (dpo@aecc.ac.uk).

4.3 The AECC Data Protection Breach Reporting Form shall be used to report all breaches and Near Misses within the AECC University College.

4.4 Information Governance incidents raised in AECC Clinics via Significant Event Reporting Forms (SERF2) may be elevated from clinic minor incident reporting process to the AECC University College Data Protection Breach Reporting Log if the event is evaluated as a medium to high risk concern.

4.4.1 Elevation to the AECC University College Data Protection Breach Reporting Log will be decided by the DPO in consultation with the relevant Clinic Director.

4.2 The Data Protection Breach Report must include:

- full and accurate details of the incident,

- when the breach occurred (dates and times),
- who is reporting it,
- if the data relates to people, the nature of the information, and
- how many individuals are involved.

5. Containment and recovery

5.1 The Data Protection Officer (DPO) will take immediate steps to prevent any further or ongoing damage resulting from the breach.

5.2 An initial assessment will be made by the DPO in liaison with the Chief Operating Officer and/or the appropriate departmental head or Caldicott Guardian as required to:

- establish the severity of the breach
- assign to the lead to investigate the breach. (This will depend on the nature of the breach; but in most cases it would be the DPO).

5.3 The investigation will establish any possible actions required to recover any losses and limit damage real or potential.

5.4 The investigation will establish who may need to be notified as part of the initial containment.

5.5 Advice from colleagues from across the University College and relevant external sources such may be sought in resolving the incident promptly.

5.6 The DPO, in liaison with relevant colleagues will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1 An investigation will be undertaken by the DPO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

6.2 The DPO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

6.3 The investigation will need to take into account the following:

i. The types of data involved
ii. its sensitivity;
iii. the protections that are in place (e.g. encryptions);
iv. what has happened to the data (e.g. has it been lost or stolen);
v. whether the data could be put to any illegal or inappropriate use;
vi. data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)

vii. whether there are wider consequences to the breach.

7. Notification

7.1 The DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

7.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered:

i. whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under the GDPR;

ii. whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);

iii. whether notification would help prevent the unauthorised or unlawful use of personal data;

iv. whether there are any legal / contractual notification requirements;

v. the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

7.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with information on how they can contact the University College for further information or to ask questions on what has occurred.

7.4 The DPO must consider notifying third parties such as the police, insurers, banks or credit card companies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.5 The DPO will consider whether the Marketing and Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

7.6 A record will be kept of any personal data breach, regardless of whether notification was required.

AECC University College

8 Evaluation and response

8.1 Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3 The review will consider:

i. where and how personal data is held and where and how it is stored;
ii. where the biggest risks lie including identifying potential weak points within existing security measures;
iii. whether methods of transmission are secure; sharing minimum amount of data necessary;
iv. staff awareness;
v. implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4 If required, a report recommending any changes to systems, policies and procedures will be considered by the University College's Senior Management Group.

Version:	2.
Approved by:	SMG
Originator/Author:	Chief Operating Officer (COO)/Data Protection Officer (DPO)
Owner:	Data Protection Officer (DPO)
Reference Source:	COI templates and guidelines
Date Approved:	June 2018
Effective From:	June 2018
Review Date:	June 2021
Target:	Staff, students, patients, public
Policy location:	SIP, Moodle, Training portals, Website
Equality analysis	This Policy has been developed with regard to the University College's general equality duty.

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, you must notify the DPO (dpo@aecc.ac.uk).

Section 1: Notification of Data Security Breach	**To be completed by the member of staff who discovered or witnessed the breach**
Date incident was discovered:	
Date incident reported if different from above	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Clinic patient number, staff number or student Id number of data subject(s) affected.	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	

Section 2: Assessment of Severity	**To be completed by the DPO in consultation with the COO and relevant colleagues**
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University College or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data • **Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to vulnerable adults and children;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	

• Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals.	
• Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	**To be completed by Data Protection Officer**
Incident number	**e.g. year/001**
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Has all appropriate action been completed to mitigate further breach?	
Does Incident need to be added to departmental/organisational/ Risk Register?	
Follow up action required/recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Officer:	
Notification to ICO	**YES/NO If YES, notified on:** **Details:**

Notification to data subjects	**YES/NO If YES, notified on:** **Details:**
Notification to other external, regulator/stakeholder	**YES/NO If YES, notified on:** **Details:**