DATA BREACH POLICY

Version: Acuity Data Breach Policy 2021.Docx
Last Reviewed: 11 November 2020
Next Review: 31 December 2021

Contents

1 Introduction

Acuity holds, processes, and shares a large amount of personal data, a valuable asset that needs to be suitably protected.

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

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs

2 Purpose

Acuity is obliged under the Data Protection Act to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the business

3 Scope

This Policy relates to all personal and sensitive data held by Acuity regardless of format.

This Policy applies to all Acuity staff and associates. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of Acuity.

The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4 Definition / types of breach

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately and has caused or has the potential to cause damage to Acuity's information assets and/or reputation.

An incident includes but is not restricted to, the following:

- 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)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

5 Reporting an incident

Any individual who accesses, uses or manages Acuity's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer and the Director responsible for IT (see Appendix II below for current names and contact details of all key roles).

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report will 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. An Incident Report Form should be completed as part of the reporting process. (See Appendix I).

All staff should be aware that any breach of the Data Protection Act may result in Acuity's Disciplinary Procedures being instigated.

6 Containment and recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant officers to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

7 Investigation and risk assessment

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

The LIO 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.

The investigation will need to take into account the following:

- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach

8 Notification

The LIO and / or the DPO, in consultation with the Director(s) responsible for IT and for Governance and Registry Services, will determine who needs to be notified of the breach.

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

- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?
- Would notification help the University meet its obligations under the seventh data protection principle;
- If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/for-organisations/report-a-breach/ (accessed 10/11/20)
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Notification to the individuals whose personal data has been affected by the incident 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 a way in which they can contact the University for further information or to ask questions on what has occurred.

The LIO and or the DPO must consider notifying third parties such as the police, insurers, bank or credit card companies, and trade unions. 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.

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

All actions will be recorded by the DPO.

9 Evaluation and response

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.

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.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by University Executive Committee.

10 Allegations of a breach by a third party

It is possible a data breach allegation could be made by a third party (e.g. a tenant). If so, details of the person making the allegation and full details of the circumstances surrounding what they perceive to be the breach should be noted.

The issue should be fully investigated in line with Acuity's Data Breach Policy. If a breach is identified, steps outlined in this policy should be followed. If no breach is identified, a formal reply should be provided to the complainant explaining why a data breach has *not* occurred. Depending upon the circumstances associated with the reporting of the allegation, the formal reply may be made directly from Acuity or, if appropriate, from a third party (for example, in instances where a tenant makes an allegation to a landlord, and the landlord is corresponding with the tenant). Copies of all correspondence should be kept on the Data Protection section of the file system.

11 Appendix I

11.1 Data breach report form

To be completed by the person reporting incident

Please act promptly to report any data breaches. If you discover a data breach, please notify a Director immediately, complete Section 1 of this form and email it to the Data Protection Officer and the Director responsible for IT

Date incident was discovered:	
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:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

12 Appendix II – Contact details

Data Protection Officer

Denise Raine

denise.raine@arap.co.uk

Director responsible for IT

Mark Anderson

mark.anderson@arap.co.uk