

could cause.

- 4.4 The investigating officer will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.
- 4.5 The investigating officer, in liaison with the Data Breach Group will determine the suitable course of action to be taken to ensure a resolution to the incident.

5. Investigation and Risk Assessment

- 5.1 An investigation will be undertaken by the nominated investigating officer immediately and wherever possible within 24 hours of the breach being discovered/reported.
- 5.2 The investigating officer 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.
- 5.3 The investigation will need to take into account the following:
 - the type and sensitivity of the data involved
 - any protections in place (e.g. encryptions)
 - what has happened to the data e.g. has it been lost or stolen
 - whether the data could be used

if a large number of people are affected, or there are very serious consequences, whether the Information

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/media/1536/breach_reporting.pdf the dangers of over notifying, not every incident warrants notification and over notification may cause disproportionate enquiries and work.

6.3

staff awareness
implementing a data breach plan and identifying a group of
individuals responsible for reacting to reported breaches of
security

- 7.4 If deemed necessary a report recommending any changes to systems, policies and procedures will be prepared for consideration by Strategic Management Team.

DATA BREACH GROUP

Douglas Hendry, Executive Director, Customer Services (01546 604244)

Charles Reppke, Head of Governance and Law (01546 604192)

Judy Orr, Head of Customer and Support Services (01586 555280)

Iain Jackson, Governance and Risk Manager (01546 604188)

Gerry Wilson, ICT and Digital Manager (01436 658936)

Andy Hubbard, ICT Compliance and Security Officer (01436 658980)

John McVey, ICT Production Manager (01546 604486)

Katrina Duncan, ICT Project and Liaison Manager (01436 658938)

Gerry McDonald, ICT Networks and Server Manager (01436 658979)

Kate Connelly, Solicitor (01546 604166)

APPENDIX 1: DATA BREACH REPORT FORM

Please act promptly to report any data breaches.

If you discover a data breach, you must;

notify your line manager immediately
the line manager must complete Section 1 of this form
email it to databreach@argyll-bute.gov.uk

Section 1: Notification of Data Security Breach	To be completed by officer reporting the incident
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:	

Nu

To be completed by Governance and Law	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by the Investigating Officer in consultation with the in liaison with the Data Breach Group
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 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:

