



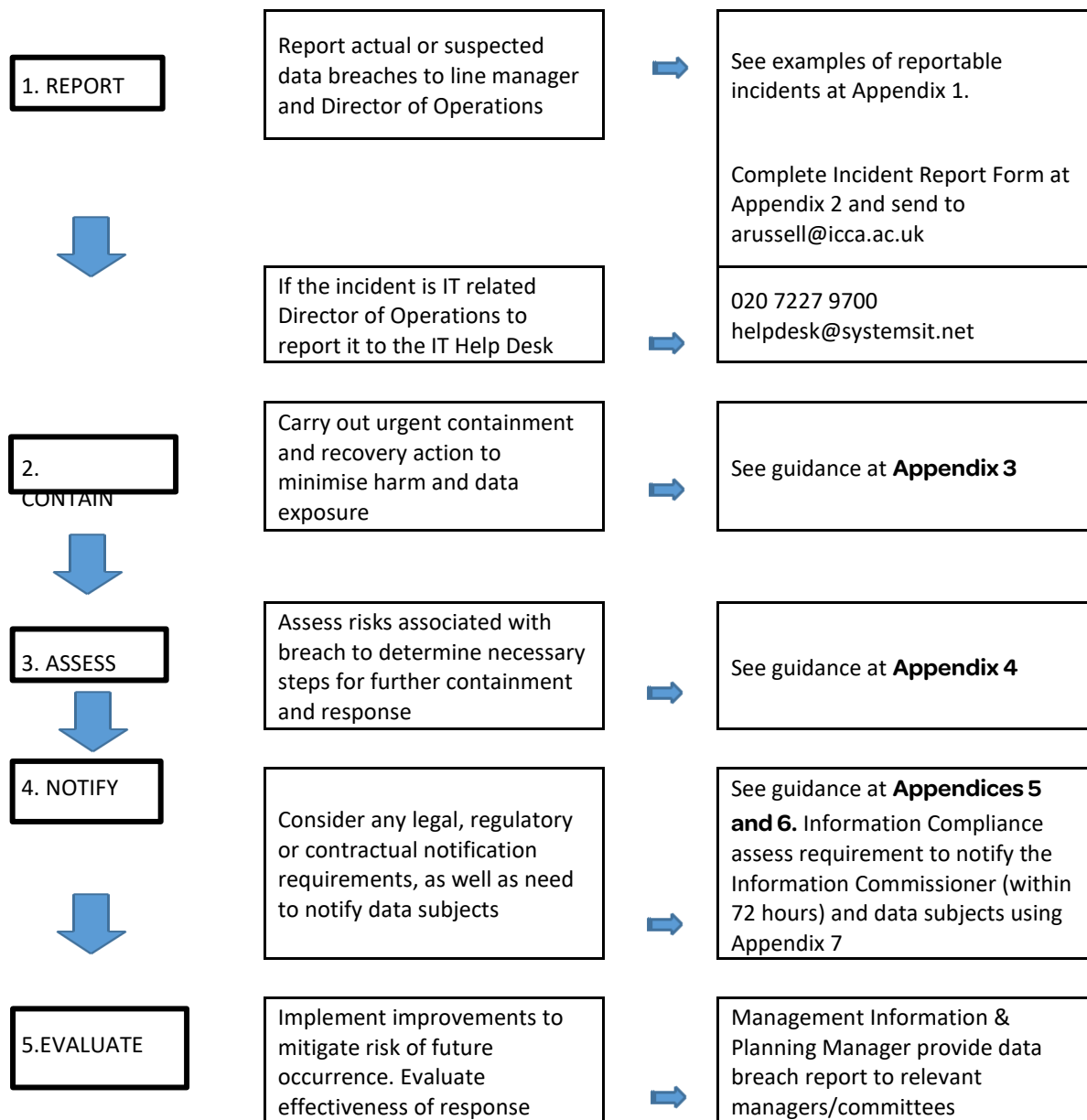
The Inns of  
Court College  
of Advocacy

# Data Breach Management Procedure

# Contents

ICCA Data Breach Management Procedure.....	1
1. Process flowchart.....	3
2. Introduction.....	3
3. Purpose.....	4
4. Definitions.....	4
5. Roles and responsibilities.....	5
6. Breach Management Process.....	8
8. Data breach evaluation.....	9
Appendix 1: Examples of Incidents Which Should Be Reported (Step 1: Report).....	10
Theft.....	10
Malicious intent.....	10
Malfunctions.....	10
Appendix 2: Data Breach Incident Report Form (Step 1: Report).....	11
Appendix 3: Containment and Recovery Checklist (Step 2: Contain).....	14
Appendix 4: Assessment of Risks Checklist (Step 3: Assess).....	16
Appendix 5: Notification Requirements Checklist (Step 4: Notify).....	17
Appendix 6: Example Notification to Data Subject (Step 4: Notify).....	20
Appendix 7: Severity Assessment Tool (Step 4: Notify).....	21
Appendix 8: Evaluation and Response Checklist (Step 5: Evaluate).....	23
Appendix 9: Data Breach Activity Log.....	24

## 1. Process flowchart (note: although presented sequentially, steps may occur concurrently)



## 2. Introduction

2.1 The Inns of Court College of Advocacy relies on a significant amount of personal data. Information about our current and prospective students, employees, and alumni are essential to our day-to-day operations.

2.2 Care needs to be taken to protect this information from loss or unauthorised destruction, alteration, disclosure or access, whether due to human error or malicious intent.

2.3 Under data protection legislation, the college must take appropriate organisational and technical measures to prevent such data breaches. Failure to do so can lead to fines of up to €20 million or 4% of annual global turnover (whichever is higher).

2.4 As well as administrative fines, data protection legislation also provides affected individuals with a right to receive compensation for the damage suffered. Furthermore, data breaches are likely to lead to adverse publicity for, and a loss of trust in the college.

2.5 All members of the ICCA including staff, students and others acting for or on behalf of The Inns of Court College of Advocacy are responsible for safeguarding the personal data they process, in

accordance with the ICCA's Data Protection Policy, of which this Personal Data Breach Management Procedure ("this Procedure") forms a part.

2.6 The Director of Operations may recommend the instigation of the relevant disciplinary procedure for staff, or misconduct procedure for students, where evidence of non-compliance with the Data Protection Policy is brought to light under this Procedure.

2.7 Non-compliance with this Procedure itself, including hindering or causing unnecessary delay to an investigation, may result in disciplinary action in accordance with the appropriate disciplinary procedures.

### **3. Purpose**

3.1 The purpose of this Procedure is to standardise the ICCA's response to any reported personal data breach incident, and ensure all incidents are managed in accordance with legal and regulatory requirements and best practice guidelines.

3.2 The implementation of this Procedure will ensure that:

- 3.2.1 incidents are reported and properly managed in a timely manner;
- 3.2.2 normal operations are restored as soon as possible;
- 3.2.3 incidents are handled by appropriately authorised and skilled staff members;
- 3.2.4 incidents are suitably recorded and documented;
- 3.2.5 the impact of data breaches is understood, and action is taken to prevent further damage;
- 3.2.6 external bodies and individuals are informed as required; and
- 3.2.7 incidents, and the ICCA's response, are subsequently reviewed to identify improvements in policies and procedures (including this one) to help mitigate the risk of further occurrence.

### **4. Definitions**

4.1 Data breach: this is defined in Article 4(12) of the General Data Protection Regulation as: 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.' Examples of data breaches are included in Appendix 1.

4.2 Data subject: the individual to whom the personal data relates.

4.3 Personal data: any information relating to an identifiable person who can be directly or indirectly identified.

4.4 Sensitive/special category personal data: the following types of personal data (specified in data protection legislation) which are particularly sensitive and private in nature, and therefore more likely to cause distress and damage if compromised:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any criminal offence
- Biometric data where processed to uniquely identify an individual

## 5. Roles and responsibilities

5.1 Table of roles and responsibilities:

<b>Role in breach management</b>	<b>Responsibility</b>	<b>Person/role within ICCA's</b>
Staff who experience or discover an incident which appears to be a data breach	<p>Know to whom they should report or escalate an incident.</p> <ul style="list-style-type: none"> <li>•This will normally be their line manager. The line manager should report the incident to the Director of Operations</li> </ul>	Any relevant staff member
	<p>The IT Service Desk should ensure that incidents which are reported to them are notified to Director of Operations without delay where personal data is involved. This could include lost or stolen IT equipment or devices, or unauthorised access to systems.</p>	•IT Service Desk staff
Students who experience or discover an incident which appears to be a data breach	<p>Report incidents to their tutor or supervisor, who will be responsible for onward reporting of the incident to the relevant Director of Operations</p>	Any relevant student
'Incident Owner'	<p>Primary responsibility for managing the breach in accordance with this Procedure.</p> <p>The 'Incident Owner' must not be the same person who experienced/discovered the data breach.</p>	Director of Operations or nominated deputies
'Responsible Staff Member'	<p>Primary day to day responsibility for the data which has been compromised, and may also be the person who experienced or</p>	Any relevant staff member

	<p>discovered the breach.</p> <p>The 'Responsible Staff Member' plays an important role in providing information about the data which has been compromised.</p> <p>In some circumstances this person may be an affiliate or a contractor.</p>	
<p><b>'Incident Response Team'</b></p> <p>Note: this is a suggested team of individuals likely to be required to deal with more serious and complex, but <b>not critical</b>, data breaches.</p> <p>See paragraph 6.7 for details of how to deal with critical incidents under the ICCA's business continuity plans.</p> <p>Expert advice on this Procedure and data protection requirements</p>	<p>Convened where necessary and is responsible for assisting the 'Incident Owner' in managing the breach.</p> <p>Where necessary, the 'Incident Response Team' should convene as soon as possible after the data breach occurs.</p> <p>Logging all breaches</p> <p>Advising on all aspects of this Procedure and related matters</p> <p>Assessing the need to notify the Information Commissioner's Office and data subjects</p> <p>Producing a data breach report with recommended actions</p>	<p>'Incident Owner' Responsible Staff Member and other relevant staff as required</p> <p>IT</p> <p>Director of Operations</p> <p>Management Information &amp; Planning Manager</p>
<p>Expert advice on communications regarding the data breach</p>	<p>Formulating messages to media and other external parties</p> <p>Dealing with press enquiries</p>	<p>Director of Operations</p>

	Drafting internal messages on the breach	
Knowledge and management of IT systems and security controls	Helping identify what information has been compromised  Implementing mitigating actions to contain and recover electronic data, equipment and devices	Director of Operations Management Information & Planning Manager IT
Knowledge and management of building security controls	Helping identify what information has been compromised  Implementing mitigating actions to contain and recover data, equipment, devices stolen from ICCA's buildings	External - Estates Security Director of Operations
Knowledge and management of staff data	Helping identify what staff information has been compromised	Director of Operations
Legal advice	Advising where there is a risk of legal action or general legal advice is required	External solicitors Director of Operations
Notifying and liaising with the Information Commissioner's Office	Deciding whether the criteria for notifying the ICO under the General Data Protection Regulation have been met	Director of Operations

5.2 Data breach incidents may occur because of, or relating to, major IT incidents which are managed by external IT Providers. Where this occurs, the ICCA's and IT's procedures shall run in parallel (with this Procedure identifying the management steps to address the breach of personal data), but the 'Incident Owner' under this Procedure shall be the IT Provider.

## 6. Breach Management Process

6.1 All data breaches must be reported as a matter of urgency in accordance with the reporting protocols in 5.1 and 5.2. See **Appendix 1** for examples of incidents that should be reported and **Appendix 2** for the Incident Report Form.

6.2 It is important that data breaches are reported to Director of Operations (arussell@icca.ac.uk) immediately so that the seriousness of the breach and further notification requirements can be determined as soon as possible.

**The ICCA has a statutory duty to inform the Information Commissioner's Office within 72 hours of becoming aware of any data breach that is likely to result in a risk to the rights and freedoms of individuals. Failure to do so can lead to a fine of up to €10m or 2% of annual global turnover (whichever is higher).**

6.3 IT related incidents should also be reported to the Director of Operations in the first instance who will inform the IT Help Desk (020 7227 9700; [helpdesk@systemsit.net](mailto:helpdesk@systemsit.net)).

6.4 Once a data breach has been reported, its management has four key elements:

6.4.1 **Containment and recovery** to limit damage as far as possible.

6.4.2 **Assessment of risks** to help inform decisions about remedial actions and notification.

6.4.3 **Notification** to the appropriate bodies/individuals that a breach has occurred.

6.4.4 **Evaluation** of the causes of the incident and the effectiveness of the ICCA's response, identifying lessons to be learned.

6.5 Suggested actions and points for consideration when addressing the four strands in 6.4 are given in the supporting appendices.



- 6.6 Depending upon the seriousness and complexity of the breach, an 'Incident Response Team' may be established, comprising appropriate ICCA's expertise (see suggested members in 5.1) to ensure that the incident is managed effectively.
- 6.8 Unless obliged under a legal, contractual or regulatory duty, any discussion of the data breach (including the fact that a breach has occurred) must be restricted to those directly involved in the investigation. Wider notification must be agreed by the 'Incident Owner', 'Incident Response Team' or Director of Operations.
- 6.9 Processors (third party companies providing services on ICCA's behalf) are legally obliged to notify the ICCA of all data breaches under Article 33(2) of the General Data Protection Regulation. Notification must be without undue delay after the processor becomes aware of the breach.

## **8. Data breach evaluation**

- 8.1 The data breach may highlight remedial action which is required in relation to procedures, training requirements, IT systems or the breach management process itself. Any agreed actions and target dates for completion will be recorded in a data breach report.
- 8.2 Director of Operations will draft the data breach report and:
  - 8.2.1 liaise with the 'Incident Owner' to ensure that departmental actions are completed
  - 8.2.2 escalate any actions that have not been completed by the target date
  - 8.2.3 ensure that guidance material is revised to reflect any learning outcomes; and
  - 8.2.4 report all data breaches to Audit and Risk Committee for monitoring and oversight.

# APPENDIX 1: EXAMPLES OF INCIDENTS WHICH SHOULD BE REPORTED (STEP 1: REPORT)

Use the Incident Report Form (Appendix 2) for the following types of incidents or similar.

If in doubt, report it.

- Human error
- Personal data emailed, posted or handed to the wrong recipient
- Excessive/non-essential personal data provided to otherwise valid recipients
- Personal data received in error
- Loss of hard copy material containing personal data
- Loss of any ICCA-owned\* data storage device, regardless of the data it contains, e.g. laptop, PC, USB drive, tablet, removable hard drive, smart phone or other portable device
- Unauthorised publication of personal data onto a website or social media channel

\*Loss of any privately-owned devices should only be reported if they contain personal data related to ICCA's activities

## Theft

- Theft of hard copy material containing personal data
- Theft of any ICCA-owned\* data storage device, regardless of the data it contains, e.g. laptop, PC, USB drive, tablet, removable hard drive, smart phone or other portable device

\*Theft of any privately-owned devices should only be reported if they contain personal data related to ICCA's activities.

## Malicious intent

- Attempts (either failed or successful) to gain unauthorised access to ICCA's systems, e.g. hacking
- Virus or other malicious malware attacks (suspected or actual)
- Compromised user accounts, e.g. disclosure of user login details through phishing
- Information obtained by deception ("blagging")
- Deliberate leaking of personal data

## Malfunctions

- Failure of software or hardware leading to personal data loss
- Damage or loss of personal data due to fire, flood, power surge or other physical damage

## APPENDIX 2: DATA BREACH INCIDENT REPORT FORM (STEP 1: REPORT)

On discovery of an actual or suspected data breach, immediately notify your line manager and/or the Director of Operations.

Following this, please complete this incident report form as soon as possible following the discovery of the incident. Please submit even if you are unable to complete the entire form – missing answers can be provided as and when the information becomes available. The questions on the form are also designed to assess the nature and likely impact of the breach which will help with each of the steps of the data breach management process. You may find it useful to read the assessment of risks guidance at Appendix 4 of the Personal Data Breach Management Procedure.

Please note that circulation of this form and any related documents must be restricted to those directly involved in investigating the incident. Please do not refer to any data subjects by name in this report.

<b>1. Your details</b>	
Report completed by [name, job title, team/department]	
Telephone	
Email	
Date of report	
<b>2. Details of the data breach – questions in red must be answered in the initial report</b>	
<b>(a) Time and date breach was identified and by whom</b>	
<b>(b) Description of incident – include time, date, location, how the incident occurred etc</b>	
<b>(c) If there has been a delay in reporting this incident please explain your reasons for this</b>	
(d) Details of any 3rd party service providers involved in the breach	

(e) What measures were in place to prevent an incident of this nature occurring (e.g. encryption, back-ups, procedures, training)	
(f) Please provide extracts/links to any policies and procedures considered relevant to this incident	
<b>3. Personal data compromised – questions in red must be answered in the initial report</b>	
<b>(a) Type of personal data compromised (provide examples/as much detail as possible)</b>	
<b>(b) Sensitive personal data<sup>1</sup> compromised (specify which, if any)</b>	
<b>(c) Potential adverse consequences for the individuals – what are they, how serious or substantial are they and how likely are they to occur?</b>	
(d) Number of individuals whose personal data has been compromised	
(e) Volume of data/records involved	
(f) Type of individuals whose data has been compromised (e.g. students, staff, job applicants)	
(g) Are the affected individuals aware that the incident has occurred?	
(h) Have any affected individuals complained about the incident?	
<b>4. Containment and recovery – questions in red must be answered in the initial report</b>	
<b>(a) Is the breach contained or ongoing?</b>	
<b>(b) What steps were/will be taken to contain the breach?</b>	
<b>(c) When was the breach contained?</b>	
<b>(d) If data lost or stolen, what steps are being taken to recover the data? If already recovered, when was the data recovered?</b>	
(e) Who has been informed of the breach (both inside and outside of ICCA)?	
(f) Details of regulatory bodies or collaborative partners who may need to be informed (e.g. BSB)	
(g) Has there been any media coverage of the incident? If so provide details	
<b>5. Training and mitigating recurrence</b>	

(a) Has the person(s) responsible for or involved with the breach completed and passed the ICCA's mandatory Data Protection e-learning module? If so, when was this completed?	
(b) What steps can be taken to minimise the possibility of a repeat of such an incident?	
<b>-- To be completed by Director of Operations</b>	
Incident Reference:	
<p><b>Incident severity rating based on assessment tool at Appendix 7:</b></p> <p>Breakdown calculation of score, including relevant sensitivity factors applied</p>	
<p><b>Overall assessment – likely to result in:</b></p> <p><b>(a) no risk to the data subject;</b></p> <p><b>(b) risk* to the data subject; or</b></p> <p><b>(c) high risk** to the data subject?</b></p> <p>Provide brief explanation for decision.</p> <p>*Risk = must notify ICO</p> <p>**High risk = must notify data subject</p>	

1 Sensitive personal data is specifically: race/ethnicity, political/religious beliefs, Trade Union membership, physical/mental health or condition, sexuality/sex life, criminal offence, biometric data where processed to uniquely identify an individual. For the purposes of data breach management, other information such as bank account details should also be classed as sensitive due to the risk of fraud

## APPENDIX 3: CONTAINMENT AND RECOVERY CHECKLIST (STEP 2: CONTAIN)

	Step	Possible actions
1	Establish 'Incident Owner' and 'Incident Response Team' as necessary	<p>Director of Operations</p> <p>or their nominated deputy to take the lead</p> <p>in investigating the extent and nature of the breach, and to contact and co-ordinate with the 'Incident Response Team' members as necessary (see 5.1 for roles and responsibilities):</p> <ul style="list-style-type: none"> <li>• Responsible Staff Members</li> <li>• Marketing</li> <li>• IT - external</li> <li>• Legal - external</li> </ul>
2	Ensure that any possibility of further data loss is removed or mitigated as far as possible.	<p>Change passwords or access codes</p> <p>Isolate/close part of network</p> <p>Take down webpages</p> <p>Restrict access to systems to a small number of staff until more is known about the incident</p> <p>Inform building security so appropriate additional physical measures can temporarily be put in place</p>
3	Determine whether anything can be done to recover any losses	<p>Physical recovery of lost data/equipment – inform security/check relevant lost property offices</p> <p>Physical recovery of stolen data/equipment – inform security and the police as appropriate</p> <p>Use back-ups to recover corrupted data</p>
		Recall incorrectly sent emails. If the recall is unsuccessful try contacting the person(s) to whom the data has been disclosed, apologising and asking them to delete the email from their systems (including from deleted items folders) and to confirm that they have done so
		Retrieve paper documents from any unintended

		recipients
4	<p>Ensure all key actions and decisions are logged and recorded on the Data Breach Activity Log (<b>Appendix 9</b>)</p>	<p>Complete the Data Breach Activity Log at each stage of the process to keep an evidence and audit trail of the breach and the remedial action taken.</p> <p>This will be important for evaluation and for demonstrating compliance to the Information Commissioner's Office</p>

## APPENDIX 4: ASSESSMENT OF RISKS CHECKLIST (STEP 3: ASSESS)

Note: if you have already completed the Data Breach Incident Report Form (Appendix 2) in full, you should have already considered most of this checklist.

1	What type and volume of personal data is involved?	
2	How sensitive is the data?	"Sensitive personal data" as specified in 4.4 of this Procedure, but also sensitive information such as bank account details due to the risk of fraud
3	What has happened to the data?	Has it been lost, stolen or damaged? If the data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate. If the data has been damaged, this poses a different type and level of risk
4	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device
5	If the data was damaged/corrupted/lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies
6	How many individuals' personal data are affected by the breach?	
7	Who are the individuals whose data has been compromised?	E.g. students, applicants, staff, customers, clients or suppliers
8	What could the data tell a third party about the individual? Could it be misused?	Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
9	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: physical safety; emotional wellbeing; reputation; finances; identity (theft/fraud from release of non-public identifiers); or a combination of these and other private aspects of their life?
10	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
11	Are there others who might advise on risks/courses of action?	E.g. if individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help prevent fraudulent use



# APPENDIX 5: NOTIFICATION REQUIREMENTS CHECKLIST (STEP 4: NOTIFY)

Notification can be an important part of the breach management process, but notification must have a clear purpose.

1	Are there any legal, contractual or regulatory requirements to notify?	E.g. terms of funding; contractual obligations
2	Can notification help the ICCA meet its security obligations under data protection legislation?	E.g. prevent any unauthorised access, use or damage to the information or loss of it
3	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their accounts)?
4	If there is a high risk to individuals, there is a legal requirement to notify those individuals <b>without undue delay</b>	The requirement to notify individuals does not apply if: <ul style="list-style-type: none"> <li>the personal data concerned was protected with appropriate technical and organisation measures (e.g. encryption);</li> <li>the ICCA has taken steps which ensure 'high risk' unlikely to materialise (e.g. lost data has been retrieved or compromised passwords reset); or</li> <li>it would involve disproportionate effort (but a public communication or similar is required instead)</li> </ul>
5	If there is a risk to individuals, there is a legal requirement to notify the Information Commissioner's Office <b>without undue delay and (where feasible) within 72 hours</b> of becoming aware of the breach	Contact and liaise with Director of Operations
6	Consider the dangers of over-notifying	E.g. notifying 100 students of an issue affecting only 10 students may well cause unnecessary concern and a disproportionate

		number of enquiries
7	<p>Consider whom to notify, what you will tell them and how you will communicate the message</p>	<p>• There are several different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation.</p> <p>• Consider how notification can be made appropriate for different groups of individuals (e.g. children, staff, research subjects, students)</p> <p>• Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done and/or what will be done to respond to the risks posed by the breach.</p> <p>• When notifying individuals, give specific and clear advice on the steps they can take to protect themselves and what the ICCA is willing to do to help them.</p> <p>• Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or FAQs on a web page). Also include contact details for the ICCA's Data Protection Lead (arussell@icca.ac.uk).</p> <p>Contact External Relations and Internal Communications as appropriate for advice. See example notification at Appendix 6.</p>
8	<p>Consider the need to notify any third parties who can assist in helping or mitigating the impact on individuals</p>	<p>E.g. police, lost property offices, insurers, professional bodies, funders, trade unions,</p> <p>website/system owners, bank/credit card companies</p>



# APPENDIX 6: EXAMPLE NOTIFICATION TO DATA SUBJECT (STEP 4: NOTIFY)

Dear [data subject's name]

## What happened?

I am writing to inform you that, regrettably, an unencrypted mobile device containing some of your personal information and in the possession of The Inns of Court College of Advocacy has been [misplaced on public transport].

## What information was involved?

The information relates to a [copy of your application form when you applied for a role at the ICCA] and therefore contains information such as [your address, telephone, email and national insurance number].

[There is no suggestion to date that the device has been found and used for malicious purposes and it may have been handed in to lost property, but it has not so far been retrieved.]

## What we are doing

On behalf of The Inns of Court College of Advocacy, I would like to apologise unreservedly for this incident. Measures have been taken to ensure that the breach has been contained, no further local copies of the data are held and that no further incidents will occur. A full investigation is underway. [The incident has been reported to the police].

## What you can do

It is important, however, to be vigilant and we would recommend reviewing the advice provided by the Information Commissioner's Office on their website for this type of circumstance:  
<https://ico.org.uk/for-the-public/identity-theft/>.

## For more information

If you have any questions about this incident, or what to do next, please reply to me by email. You can also contact the ICCA's Data Protection Lead, at [TBC]

With sincere apologies once more.

Yours faithfully

[Name, job title, contact details]

## APPENDIX 7: SEVERITY ASSESSMENT TOOL (STEP 4: NOTIFY)

The tool below is intended as a guide only and should not be relied on to reflect all relevant circumstances. Director of Operations will assess the severity of a breach on a scale of 0-3. An incident scoring 3+ may be considered 'high risk' and therefore require notification to data subjects without undue delay in accordance with the General Data Protection Regulation. The Director of Operations should be consulted for a final decision on notification to data subjects.

No. of individuals whose data has been disclosed or put at risk	0	1	2	3
0-11				
12-100				
101-1,000				
1,001 plus				

Sensitivity factors should be applied to the initial score as follows:

**For each of the following sensitivity factors reduce score by 1 (not applicable in the case of a score of 0)**

- A. No sensitive personal data
- B. Information already accessible or in public domain
- C. Low level of harm to individuals

**For each of the following factors increase score by 1**

- D. Detailed information at risk e.g. medical documentation notes
- E. High risk confidential information
- F. One or more previous similar incidents in last 12 months
- G. Failure to implement, enforce or follow technical safeguards to protect information
- H. Likely to attract media interest or other reputational damage and/or a complaint has been made to the ICO by an organisation or individual
- I. Individuals are likely to suffer substantial damage or distress including significant embarrassment or detriment
- J. Individuals likely to have been placed at risk of physical harm

Sensitivity factors which would not be relevant should be excluded as follows.

When user selects this...	...the following sensitivity factors are excluded
A	D, E

B	D,E,I,J
C	I, J
D	A, B
E	A, B
F	None
G	None
H	None
I	B, C
J	B, C

## APPENDIX 8: EVALUATION AND RESPONSE CHECKLIST (STEP 5: EVALUATE)

1	Establish where any present or future risks lie	
2	Consider the data and contexts involved	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept
3	Consider and identify any weak points in existing security measures and procedures	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections
4	Consider and identify any weak points in levels of security awareness/training	Fill any gaps through training or tailored advice
5	Report on findings and implement recommendations	Report to Director of Operations, other relevant staff members

## APPENDIX 9: DATA BREACH ACTIVITY LOG

Date/Time	Activity Activity, Decision, Instruction or Briefing (A, D, I or B)	Action	Owner	Completed
E.g. 08/01/20, 12.20pm	B – received notification of personal data available on website	Informed web team and requested page to be taken down immediately	M.Fligler	2.30pm

**Completed  
by:**