Step	*Action points*	*Notes*
	Containment and recovery	**To contain any breach, to limit any further damage as far as possible and to seek to recover any lost data or equipment.**
1	Establish a lead for investigating breach	To investigate extent and nature of breach, to contact and co-ordinate with specialists and stakeholders (for example Data Protection specialist, central IT Services, College IT Manager, system owners, External Relations).
2	Ensure lead has appropriate resources	Including sufficient time and authority.
3	Ascertain the scope of the breach and if any personal data is involved.	**See Risk assessment below**
4	Establish who needs to be made aware of the incident and inform them of what they are expected to do to assist in the containment/recovery exercise.	This may involve finding a lost piece of equipment, changing passwords or access codes, isolating/closing part of network, isolating network access port, pulling webpages, informing police. If you have any reason to suspect that there is computer misuse ('hacking'), you should contact the Information Security Officer of the ICO who will provide advice on actions to take and how to preserve evidence.
5	Ensure that any possibility of further data loss is removed or mitigated as far as possible	As above. This may involve actions such as taking computers and systems offline, or restricting access to systems until more is known about the incident.
6	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data is corrupted, through use of back-ups.
7	Where appropriate, inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
	Risk assessment	**To identify and assess the ongoing risks that may be associated with the breach. In particular: an assessment of (a) potential adverse consequences for individuals, (b) their likelihood, extent and seriousness. Determining the level of risk will help define actions in attempting to mitigate those risks.**
8	What type and volume of data is involved?	
9	How sensitive is the data?	Sensitive personal data? Of a very personal nature (e.g. health record) or sensitive because of what might happen if misused (banking details).
10	What has happened to the data?	Thus, if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
11	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	For example, encryption of data/device.
12	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	For example, back-up tapes/copies.

	Additional assessment for breaches involving personal data	
13	How many individuals' personal data are affected by the breach?	
14	Who are the individuals whose data has been compromised?	Students, applicants, staff, fellows, donors,clients or suppliers?
15	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened: Sensitive data could mean very little to an opportunistic laptop thief while the loss of trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
16	Is there actual/potential harm that could come to any individuals?	For example, are there risks to: physical safety; emotional wellbeing; reputation; finances; identify (theft/fraud from release of non-public identifiers); or a combination of these and other private aspects of their life?
17	Are there wider consequences to consider?	For example, is there a risk to public health or loss of public confidence?
18	Are there others who might advise on risks/courses of action?	If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.
	Notification	**To consider any necessary notification of people and organisations. 'Informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions'**
19	Are there any legal, contractual or regulatory requirements to notify?	Check to see if any of the information has a stated legal procedure that will need to be followed.
20	Can notification help the College meet its security obligations under the seventh data protection principle?	For example, to prevent any unauthorised access, use or damage to the information or loss of it.
21	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
22	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office (through the Director of Information).	Contact and liaise with the ICO Director of Information.
23	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying amount of people for an issue affecting only a small percentage may well cause disproportionate enquiries and work".
24	Consider whom to notify, what you will tell them and how you will communicate the message.	There are a number of different ways to notify those affected, consideration should be taken on the most appropriate method. Always bear in mind the security level as well as the urgency of the situation.

		Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. Provide a way in which they can contact specific people for further information or to ask questions about what has occurred (e.g. a contact name, telephone number or a web page).
25	Consider how notification can be made appropriate for particular groups of individuals.	E.g. vulnerable adults.
26	Consult the ICO guidance on when and how to notify it about breaches.	There is not a legal requirement to report security breaches which result in the loss, release or corruption of personal data to the Information Commissioner. Serious breaches should be brought to their attention however. Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
27	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.
	Evaluation and response	**To evaluate the effectiveness of the College's response to the breach. To learn and apply any lessons or remedies in the light of findings or experience.**
28	Establish where any present or future risks lie.	Departments and IT Committee.
29	Consider the data and contexts involved.	Thus, what data is held, its extent, sensitivity, where and how it is stored, how long it is kept).
30	Consider and identify any weak points in existing security measures and procedures.	That is, in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
31	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice. Fill in annual Security Gap or maturity analysis and carry out system risk analysis.
32	Report on findings and implement recommendations.	Report Information to the Data Protection Officer