Data Breach Management Procedure

Department of Business Assurance
Office of the Chairman & College Secretariat

Effective Date: May 2018
Last Review: August 2022

Contents

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

1. REPORT

Report actual or suspected data breaches to line manager and Director of Administration or Head of Professional Service **AND**

complete the Report a Data Breach self-service ticket which will alert both Information Compliance and IT.

→ See examples of reportable incidents at **Appendix 1**.

Complete Incident Report Form using the Report a Data Breach self-service ticket

If **NHS Digital data**, follow the NHS Digital reporting requirements

↓

2. CONTAIN

Carry out urgent containment and recovery action to minimise harm and data exposure

→ See guidance at **Appendix 3**

↓

3. ASSESS

Assess risks associated with breach to determine necessary steps for further containment and response

→ See guidance at **Appendix 4**

↓

4. NOTIFY

Consider any legal, regulatory, or contractual notification requirements, as well as need to notify data subjects, in consultation with the Information Compliance Team

→ See guidance at **Appendices 5 and 6**.

The Information Compliance Team will assess requirement to notify the Information Commissioner (ICO) within 72 hours and data subjects **using Appendix 7**

The DPO will be the university's sole point of contact with the ICO

↓

5. EVALUATE

Implement improvements to mitigate risk of future occurrence. Evaluate effectiveness of response

→ Information Compliance provide data breach report to relevant managers/committees

2. Introduction

2.1 As a large university, King's relies on a significant amount of personal data. Information about our current and prospective students, employees, research subjects, donors, 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 university must take appropriate organisational and technical measures to prevent such data breaches. Failure to do so can lead to fines of up to £17.5 million or 4 per cent of annual global turnover - whichever is greater. -

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 university.

2.5 All members of the university including staff, students and others acting for or on behalf of King's College London are responsible for safeguarding the personal data they process, in accordance with the university's Data Protection Policy, of which this Personal Data Breach Management Procedure ("this Procedure") forms a part.

2.6 The Director of Business Assurance 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 university'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 ensures 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 the 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 university'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 UK 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:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation.**

5. Roles and responsibilities

5.1 Table of roles and responsibilities:

Role in breach management	Responsibility	Person/role within King's
Staff who experience or discover an incident which appears to be a data breach	• Know to whom they should report or escalate an incident. • This will normally be their line manager or principle investigator (PI) in the context of research projects. • The line manager/PI should report the incident to the relevant	• Any relevant staff member • Information Compliance Team • IT Service Desk staff

	Director of Administration or Head of Professional Service, **AND** Information Compliance. • At any event, the **Information Compliance Team must be informed as soon as possible after a data breach is suspected.** • The IT Service Desk should ensure that incidents which are reported to them are notified to Information Compliance without delay where personal data is involved. This could include lost or stolen IT equipment or devices, or unauthorised access to systems.	
Students who experience or discover an incident which appears to be a data breach	• Report incidents to their tutor or supervisor, who will be responsible for onward reporting of the incident to the relevant Director of Administration AND Information Compliance	• Any relevant student
'Incident Owner'	• Primary responsibility for managing the breach in accordance with this Procedure. • The 'Incident Owner' must not be the same person who experienced/discovered the data breach.	• Director of Administration or Head of Professional Service, or their nominated deputies

'Responsible Staff Member'	• Primary day to day responsibility for the data which has been compromised. This may also be the person who experienced or discovered the breach. • The 'Responsible Staff Member' plays an important role in providing information about the data which has been compromised. • In some circumstances this person may be an affiliate or a contractor. If in doubt they should confirm responsibilities with the relevant King's manager.	• Any relevant staff member
Incident Response Team' Note: this is a suggested team of individuals likely to be required to deal with more serious and complex, but **not critical**, data breaches. See paragraph 6.7 for details of how to deal with critical incidents under the university's business continuity plans.	• Convened where necessary and is responsible for assisting the 'Incident Owner' in managing the breach. • Where necessary, the 'Incident Response Team' should convene as soon as possible after the data breach occurs	• 'Incident Owner' • Responsible Staff Member and other relevant staff as required • Information Compliance • PR/Internal Communications • IT • Security/Estates & Facilities • HR • Legal • (See separate role profiles)

Expert advice on this Data Breach Management Procedure and data protection requirements	• Logging all breaches • Advising on all aspects of this Procedure and related matters • Assessing the need to notify the Information Commissioner's Office (ICO) and data subjects • Notifying and corresponding with the ICO • Producing a data breach report with recommended actions, where necessary	• Director of Information Governance & DPO • Members of the Information Compliance team
Expert advice on communications regarding the data breach	• Formulating messages to media and other external parties • Dealing with press enquiries • Drafting internal messages about the breach	• Director of Corporate Communications
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, Office of the CIO • Head of IT Assurance • Head of Cyber Security
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 King's buildings	• Director of Estates & Facilities and designates depending on the building

Knowledge and management of staff data	• Helping identify what staff information has been compromised	• Director of unit • HR
Legal advice	• Advising where there is a risk of legal action or general legal advice is required	• General Counsel and Director of Legal Services
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 Information Governance & DPO

5.2 Data breach incidents may occur because of, or relating to, major IT incidents which are managed under the IT Major Incident Management Procedure. Where this occurs, the two 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 Major Incident Manager** under the IT Major Incident Management Procedure.

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** to view the Data Breach Report Form.

6.2 Data breaches must be reported to Information Compliance via the Data Breach Report Form without unnecessary delay so that the seriousness of the breach and further notification requirements can be determined as soon as possible. **The university 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 £8.7 million or 2% of annual global turnover – whichever is greater.

6.3 IT related incidents should also be reported to the IT Service Desk. Use the Data Breach Report Form to ensure your report goes to Information Compliance and IT at the same time.

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 university'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 university expertise (see suggested members in 5.1) to ensure that the incident is managed effectively.

6.7 King's has a separate, overarching Critical Incident Plan for dealing with incidents that are, or have the potential to be, detrimental to the delivery of key university activities (teaching and research). It can be activated immediately or where a data breach has escalated and has the potential to become a critical incident. Once activated, a central critical incident team will be formed and lead the university's response to a breach under its business continuity plans.

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 Senior Vice President (Operations).

6.9 Processors (third party companies providing services on King's behalf) are legally obliged to notify the university of all data breaches under Article 33(2) of the General Data Protection Regulation. Notification must be without undue delay once the processor becomes aware of the breach.

7. NHS Digital and NHS Trust data

7.1 Any data breach involving data sourced from NHS Digital must be managed in accordance with NHS Digital procedures) and reported to NHS Digital as required.

7.2 Responsibility for notification to NHS Digital will rest with the 'Incident Owner', supported by Information Compliance. Any additional requirements of the relevant NHS Digital data sharing agreement must also be fully observed.

7.3 If NHS Trust data is involved, early notification by the 'Incident Owner', supported by Information Compliance, to the relevant Trust Caldicott Guardian is required and discussions will be necessary with the Trust to determine who is the 'data controller' and whether the incident is the responsibility of the university or the Trust. Where it is determined that the incident is the responsibility of the Trust, the incident shall be passed to the Trust to manage and the incident for the university will be closed. The King's Information Compliance Team must be involved in these discussions and agree to the decision.

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 Information Compliance will draft the data breach report and:

- liaise with the ‘Incident Owner’ to ensure that departmental actions are completed;
- escalate any actions that have not been completed by the target date;
- ensure that guidance material is revised to reflect any learning outcomes; and
- report all data breaches to the university’s Information Security Steering Board and Audit Committee for monitoring and oversight.

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

Use the Data Breach Report Form 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 university-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 university activities

Theft

- Theft of hard copy material containing personal data
- Theft of any university-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 university activities.

Malicious intent

- Attempts (either failed or successful) to gain unauthorised access to university 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)

To be completed by the staff member who experiences or discovers a data breach, or their line manager, without delay.

Please use this link to access the form: Data Breach Report Form

The Data Breach Report Form should be completed as soon as possible following 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 any documents related to the incident must be restricted to those directly involved in the investigation. Please do not refer to any data subjects by name in your report.

The below is an example of the report's question fields, please do NOT use the below from to report breaches, please instead use the Data Breach Report Form

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

3. Personal data compromised – questions in red must be answered in the initial report	
(a) Type of personal data compromised (provide examples/as much detail as possible)	
(b) Sensitive personal data[1] compromised (specify which, if any)	
(c) Potential adverse consequences for the individuals – what are they, how serious or substantial are they and how likely are they to occur?	
(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, research subjects, alumni, donors, job applicants etc)	
(g) Are the affected individuals aware that the incident has occurred?	
(h) Have any affected individuals complained about the incident?	
4. Containment and recovery – questions in red must be answered in the initial report	
(a) Is the breach contained or ongoing?	
(b) What steps were/will be taken to contain the breach?	
(c) When was the breach contained?	
(d) If data lost or stolen, what steps are being taken to recover the data? If already recovered, when was the data recovered?	
(e) Who has been informed of the breach (both inside and outside of King's)?	
(f) Details of regulatory bodies or collaborative partners who may need to be informed (e.g. NHS Trust, NHS Digital)	
(g) Has there been any media coverage of the incident? If so provide details	
5. Training and mitigating recurrence	
(a) Has the person(s) responsible for or involved with the breach completed and passed the university's mandatory Data Protection e-learning module? If so, when was this completed?	

[1] Sensitive personal data is specifically: race/ethnicity, political/religious beliefs, Trade Union membership, physical/mental health or condition, sexuality/sex life, criminal offence, genetic data, 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

(b) What steps can be taken to minimise the possibility of a repeat of such an incident?	
-- To be completed by Information Compliance --	
Incident Reference:	
Incident severity rating based on assessment tool at Appendix 7: Breakdown calculation of score, including relevant sensitivity factors applied	
Overall assessment – likely to result in: **(a) no risk to the data subject;** **(b) risk* to the data subject; or** **(c) high risk** to the data subject?** Provide brief explanation for decision. *Risk = must notify ICO **High risk = must notify data subject	

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

	Step	Possible actions
1	Establish 'Incident Owner' and 'Incident Response Team' as necessary	Director of Administration/Head of Professional Service or their nominated deputy to take the lead 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): • Responsible Staff Members • Information Compliance • External Relations/Internal Communications • IT • Security/Estates & Facilities • HR • Legal
2	Ensure that any possibility of further data loss is removed or mitigated as far as possible.	Change passwords or access codes
		Isolate/close part of network
		Take down webpages
		Restrict access to systems to a small number of staff until more is known about the incident
		Inform building security so appropriate additional physical measures can temporarily be put in place
3	Determine whether anything can be done to recover any losses	Physical recovery of lost data/equipment – inform security/check relevant lost property offices
		Physical recovery of stolen data/equipment – inform security and the police as appropriate
		Use back-ups to recover corrupted data
		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	Ensure all key actions and decisions are logged and recorded on the Data Breach Activity Log (**Appendix 9**)	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. This will be important for evaluation and for demonstrating compliance to the Information Commissioner's Office

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

Note: if you have already completed the Data Breach 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. If you are considering notification, you must contact and liaise with Information Compliance first to allow them to advise you on the best course of action.

1	Are there any legal, contractual or regulatory requirements to notify?	E.g. terms of funding; contractual obligations; reporting responsibilities for researchers under the university's research misconduct policies
2	Can notification help the university 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 **without undue delay**	The requirement to notify individuals does not apply if: • the personal data concerned was protected with appropriate technical and organisation measures (e.g. encryption); • the university has taken steps which ensure 'high risk' unlikely to materialise (e.g. lost data has been retrieved or compromised passwords reset); or • it would involve disproportionate effort (but a public communication or similar is required instead) Contact Information Compliance and External Relations/Internal Communications as appropriate
5	If there is a risk to individuals, there is a legal requirement to notify the Information Commissioner's Office **without undue delay and (where feasible) within 72 hours** of becoming aware of the breach	You must contact and liaise with Information Compliance to allow them to make this assessment Notifying and corresponding with the ICO must only be done by the Director of Information Governance & DPO
6	Consider the dangers of over-notifying	E.g. notifying 30,000 students of an issue affecting only 3,000 students may well cause unnecessary concern and a disproportionate number of enquiries

7	Consider whom to notify, what you will tell them and how you will communicate the message	individuals (e.g. children, staff, research subjects, students) • 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. • When notifying individuals, give specific and clear advice on the steps they can take to protect themselves and what the university is willing to do to help them. • 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 King's Data Protection Officer (Olenka Cogias at info-compliance@kcl.ac.uk). • Contact External Relations and Internal Communications as appropriate for advice. See example notification at **Appendix 6**.
8	Consider the need to notify any third parties who can assist in helping or mitigating the impact on individuals	E.g. police, lost property offices, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies

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 King's College London 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 university 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 King's College London, 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 university's Data Protection Officer, Olenka Cogias at info-compliance@kcl.ac.uk.

With profound apologies once more.

Yours faithfully

[*Name, job title, contact details*]

APPENDIX 7: SEVERITY ASSESSMENT TOOL (FOR USE BY INFORMATION COMPLIANCE) (STEP 4: NOTIFY)

The tool below is intended as a guide only and should not be relied on to reflect all relevant circumstances. Information Compliance 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 Senior Vice President (Operations) should be consulted for a final decision on notification to data subjects.**

Where the data involved has been sourced from NHS Digital, the NHS Digital guidelines must be followed in respect of assessing the severity of the incident and reporting requirements.

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. clinical care case notes, social care 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 asfollows.

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 Administration/Head of Professional Service, other relevant staff members, the Security Operations Group, and Audit Committee

APPENDIX 9: DATA BREACH ACTIVITY LOG

Date/Time	Activity Activity, Decision, Instruction or Briefing (A, D, I or B)	Action	Owner	Completed
E.g. 08/01/18, 12.20pm	B – received notification of personal data available on website	Informed web team and requested page to be taken down immediately	J Smith	2.30pm

Completed by: