Nottinghamshire County Council

Security Incident & Breach Management Procedure

At a glance …

- A security incident / breach affects the confidentiality, integrity or availability of personal or confidential data (including the destruction, loss, alteration, disclosure of, or access to, personal data) and must be centrally reported immediately
- Line manager(s) also need to be told immediately but this should not delay reporting.
- Immediacy is required as the Council has 72 hours to report more serious breaches to Information Commissioner's Office (ICO) (the regulator for data protection) and affected individuals may need to be told sooner.
- The Information Governance Team [tel: 0115 8043800] coordinates the incident / breach procedure and provides support to departments to act swiftly to minimise harm and learn from breaches.
- Security incidents involving IT equipment, network and systems should be reported through the ICT Service desk [tel: 0115 977 2010].
- Immediate action should be taken on discovering a breach to contain and minimise its impact (e.g. retrieving / seeking the destruction of data disclosed in error). Advice will be available upon reporting.
- More serious incidents will need to be investigated to establish what went wrong and identify measures to prevent reoccurrence at a team and wider level.
- Group Managers will be advised of incidents / breaches in their areas.
- The Data Protection Officer will liaise with the Senior Information Risk Owner and Caldicott Guardian (where appropriate) to determine whether a breach should be reported to the ICO and / or data subjects.
- All incident and breaches will be logged. Quantitative and qualitative reports will be produced to support organisational learning and improvement.

Background

1. The County Council is responsible for the confidentiality, security and integrity of all information processes. It must ensure that any information security incidents which could cause damage or distress to individuals whose data the Council holds; to the Council's assets and / or reputation are prevented and/or minimised..

2. It is imperative that security incidents are reported immediately. Failure to notify immediately on discovery significantly increases risk and exposure to affected individuals and the Council.

3. This procedure forms part of the suite of documents that comprise the Council's Information Governance Framework and is a requirement of the Information Compliance Policy.

4. It is informed by the Security Incident Response Standard which is one of the collection of standards that comprises the Information Security Policy. It complements the ICT Cyber Security Response Process [being drafted - link to be inserted upon completion]

Purpose

5. The purpose of this document is to specify the procedure for the management and reporting of incidents and data breaches by the Council, ensuring that:

    a. Security incidents are dealt with quickly and efficiently.
    b. A consistent approach is applied to management and reporting of security incidents
    c. The damage caused security incidents is minimised.
    d. The likelihood of a recurrence of a security incident is reduced by the review and implementation of appropriate measures.

Scope and Definitions

6. This procedure applies to all staff including: employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information.

7. Information in this procedure is used as a collective term. The primary focus is on personal data, although most of the same considerations apply to other sensitive data, for example commercially sensitive information.

8. Information can be in any format including paper, electronic, digital images, voice recordings etc.

9. A data subject is defined as an identified or identifiable individual to whom personal data relates.

10. An an information security incident is defined as an incident that has affected the confidentiality, integrity or availability of personal or confidential data.

11. A personal data breach is an information security incident which involves personal data and is defined 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*."

12. A personal data breach is reportable where it results in risk to the rights and freedoms of data subjects. Where this is this is deemed to the case the breach must be reported within 72 hours to the Information Commissioner's Office (ICO) (the enforcement body for data protection in the UK). Such a breach may also need to be reported to other parties such as data subjects (see the notifications section of this procedure).

13. Not all incidents will be personal data breaches and not all personal data breaches are reportable.

14. Some examples of information security incidents are given in the table at paragraph 28.

15. The Council contracts with suppliers (individuals and organisations) which collect, use and store personal data on the Council's behalf as part of the services provided (e.g. care homes etc.). These suppliers will need to report security incidents to the Council without undue delay and should have in place internal reporting requirements equivalent to this procedure.

16. Likewise, the Council will need to report security incidents concerning data processed on behalf of other organisations (e.g. schools) to those organisations in accordance with the terms of the contract(s).

Principles & Commitments

17. The Council recognises that from time to time 'things go wrong' and there may be a breach of security involving information or equipment holding information.

18. The purpose of this procedure is to ensure that all information security incidents are reported centrally to enable the Council to act quickly and effectively to minimise the impact, particularly on affected data subjects. .

19. Information security incidents can cover a multitude of situations, but will generally involve an adverse event which results, or has the potential to result in the compromise, misuse or loss of Council owned or held information or assets.

20. The impact of a security incident can vary greatly depending on the type of information or asset involved. For instance, it may lead to an infringement of privacy, physical and emotional harm, fraud, financial loss, service disruption or reputational damage.

21. The purpose of reporting an incident is not to apportion blame but to ensure that any impact is minimised and lessons learnt can be identified and disseminated to minimise reoccurrences.

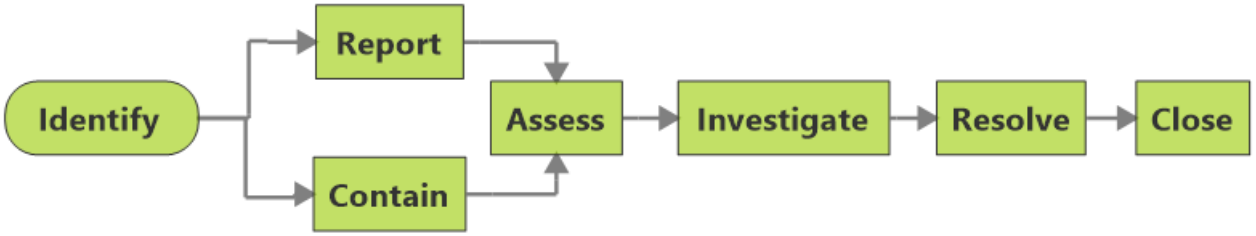
22. The principles of this procedure also apply to cyber incidents. Cyber incidents are any incidents that could or have compromised information assets within the Council's digital network (e.g. phishing emails or hacking attacks). Any cyber-related incident will be handled in accordance with the Council's ICT Cyber

Security Response Process [being drafted - link to be inserted upon completion].

23. In the event that a cyber incident also involves a personal data breach then it shall remain subject to this procedure and the Incident Lead, supported by the Information Governance Team, will work in conjunction with the ICT Security Team(s) to resolve the incident and report to regulators where necessary.

Incident Management

24. This section outlines the key stages of incident management which are:



.

Stage 1 – Incident Reporting

25. Any actual or suspected security incident must be reported immediately upon discovery. It is better to err on the side of caution and report if in doubt.

26. A direct line manager or supervisor should always be made aware of any information security incident and the incident reported in line with this procedure.

27. However, informing a line manager or supervisor of an incident must not delay any incident being reported nor should it delay taking steps to minimise the potential damage caused by the incident.

28. There are two routes for reporting security incidents within the Council, depending on the nature of the incident. These are as follows:

Security incidents involving ….	**Security incidents involving ….**
IT equipment, network and systems such as: • data changed by an unauthorised person • unknown people asking for access to council data • disclosing your password • accessing systems using someone else's user id and password	**Paper and non-IT specific incidents such as:** • unauthorised sharing of data with third parties • loss, theft or unauthorised destruction of paperwork • Information sent to the wrong recipient. • failure to redact data • verbal disclosure of information

• use of unapproved or unlicensed software on council equipment • Theft, loss or insecure disposal of council equipment (e.g. laptops, mobile phones, memory sticks, CDs etc.). • Unavailability of a key business system • sending an email containing sensitive or confidential information to 'all staff' by mistake • receiving unsolicited mail which requires you to enter personal data • Hacking / attempted hacking of data	• not using blind carbon copy (bcc) for sending emails containing personal / sensitive data • data left in an insecure location • unauthorised access granted to information • disposal of sensitive / confidential waste in recycling bins rather than confidential waste
To be reported immediately to	**To be reported immediately to**
IT Service Desk Tel: 0115 977 2010 Email (if out of office hours): itservicedesk@nottscc.gov.uk	Information Governance Team Tel: 0115 8043800 Email (if out of office hours): data.protection@nottscc.gov.uk
More information on the intranet HERE	More information on the intranet HERE

29. To address any overlaps, the ICT Service Desk and the Information Governance Team will triage calls and refer to the other, as appropriate. The ICT service Desk will liaise with the IT Security Team, depending on the severity of the incident.

30. The person reporting the incident should in the first instance telephone the ICT Service Desk or the Information Governance Team (depending on the nature of the incident) as soon as possible. They will be asked questions required to determine the risk and actions to be taken such as what happened, when it occurred, what information or assets were compromised, number of people affected and any immediate action taken to rectify the situation and minimise potential harm.

31. The person reporting the incident may, following the call, be required either to verify the details of the incident as recorded during the phone call or follow-up by completing an incident report form.

32. If the information security incident is reported outside of office hours, then a voicemail should be left and a message should be emailed to the Service Desk or the Information Governance email account and titled 'Urgent Data Incident.' An incident report form should be attached setting out as much detail as possible.

33. The Police should be notified immediately of any incidents involving stolen information or equipment and a crime reference number obtained. The individual who has had the equipment stolen is responsible for notifying the police.

34. When members of the public, information sharing partners and suppliers notify the Council of an incident they will be directed in the first instance to the Information Governance Team who will notify the Data Protection Officer and the IT Service Desk (where appropriate).

35. The incident will be logged on the Incident Logs used by the IT Service Desk / Information Governance Team.

Stage 2 – Incident Containment

36. The line manager of the member of staff who has committed a data breach should carry out actions to prevent further disclosure or damage as soon as practical.

37. For instance, in the event that information has been sent to an incorrect / unauthorised recipient, contact should be made with whoever received the information asking them either to return or delete it, depending on which is appropriate. They should also be requested to confirm that this has happened and whether the information had been further disclosed and to who.

38. Initial actions at this stage should also include ensuring that any evidence supporting the investigation of the security incident is isolated and protected.

Stage 3 – Incident Assessment

39. The severity of an incident will be determined by an incident assessment which is set out in the Incident Severity Assessment Form at Appendix A.

40. Upon notification, an initial assessment of risk will be undertaken to determine a provisional incident severity rating and appropriate internal notifications will be made as per the applicable rating.

41. Where incidents are personal data breaches and are rated as high risk consideration will be given as to whether the ICO, the affected data subject(s) and other parties should be notified.

42. This assessment will be made as soon as possible to ensure that any breach will be reported to the ICO within the 72 hour deadline where necessary. Any reporting to the ICO or other bodies will involve prior consultation by the DPO (or their nominee) with the SIRO and Caldicott Guardian (or their deputies), where appropriate.

43. An incident rating may change once the full facts and impact of risks has been determined and the status of the incident will be kept under review accordingly. In addition, this may involve updating any reports to the ICO and/or other parties accordingly.

Stage 4 – Incident Investigation & Review

44. Not all incidents will require an in depth investigation to establish the facts and determine what went wrong. However, all incidents should prompt the consideration and recommendation of measures to avoid reoccurrence and this will form part of the reporting process.

45. The level of detail provided to IT Service Desk / IT Security Team or the Information Governance Team when reporting the incident (together with any information provided in the incident reporting form when completed) should usually be sufficient to understand the incident.

46. Where the incident is assessed as being of medium or higher severity, the Group Manager of the team in which it occurred will appoint an Incident Lead to investigate the incident. For all other incidents, the line manager of the person responsible for the incident will carry out the investigation.

47. The IT Security Team and / or the Information Governance Team, as appropriate, will assign an Investigation Support Officer to assist the Incident Lead in the investigation and ensure that its findings are robust.

48. If any additional information is required then the Incident Lead will contact the person who reported the incident or any other persons involved in the incident to seek clarification or further information.

49. Where an incident is high risk and may require reporting to the ICO or any other relevant body, the DPO (or their nominee) and the IT Security Team (as appropriate) will assess the risk and identify and recommendations/actions. This will be done immediately after becoming aware of the incident and a meeting may be convened (remotely or in person) to discuss the matter.

50. The investigation should be completed and the investigation form returned by the Incident Lead as soon as possible and ordinarily no longer than 10 days after the incident occurred. Every effort should be made to conclude the investigation of more serious incidents sooner.

51. The investigation report will set out:

    (i) observations and conclusions about any information governance non-compliance issues, risks, adverse consequences or implications; and
    (ii) remedial recommendations (with owners and deadlines for completion) to mitigate the risks and impact including preventative measures; areas for improvement and training needs etc.
    (iii) It will also include the completed incident report, any additional information.

52. The competed investigation report will be reviewed by the assigned Incident Support Officer member within 5 working days but wherever possible sooner.

53. Any repeat or previous similar incidents will be flagged in the final incident report and may result in additional or escalated action.

54. The review will also take account of how well this procedure has operated and flag any scope for improvement.

55. This procedure is independent of a locally commissioned disciplinary investigation but the final incident report may inform any consequential action taken or considered.

56. Where a matter has been reported to the ICO or any other statutory body, the Incident Support Officer will continue to keep the ICO and other bodies updated on the investigation, incident review and outcome.

Stage 5 – Incident Resolution

57. The final investigation report will be sent to the relevant Group Manager to sign and accept the recommendations (within 5 working days of receipt).

58. If for any reason a recommendation is rejected then the Group Manager must specify the reasons why. Recommendations rejected by the Group Manager may be referred to the Data Protection Officer (or their nominee) for review and may prompt further discussion or escalation.

Stage 6 – Incident Closure

59. The assigned Incident Support Officer will be required to update the relevant Incident Log.

60. The Incident Support Officer will follow-up progress in completing recommended actions arising from the incident and update the log accordingly.

61. If the incident was reported to the ICO / data subject(s) or other parties, a final status and update will be recorded.

62. The DPO (or their nominee) will report incident performance to the Information Governance Board and Departmental Risk, Safety and Emergency Management Groups (RSEMGs) on a quarterly basis. This will contain both quantitative and qualitative data, providing analysis on incident trends, incident management and incident lessons learned / to be learned.

63. Reports on incident management and performance may also be produced for Council Committees.

64. An incident will only be closed when all aspects including the monitoring log updates have been completed.

Notification of incidents

Internal Notifications

65. Internal notifications will be determined in accordance with the incident rating as set out in Appendix A. The IT Service Desk or Information Governance Team will be responsible for notifications as appropriate.

66. The relevant Group Manager will be notified of all incidents that have occurred solely within their Group. They will be required to nominate an Incident Lead to investigate the more serious incidents (i.e. those assessed as medium severity or above).

67. Key senior staff (e.g. the Senior Information Risk Owner and Caldicott Guardians) will be notified of the more serious incidents (i.e. those assessed as medium severity or above).

68. In notifying the incident internally, no personal data of affected data subjects will be communicated (i.e. the material that has created the breach). Arrangements can be made for this to be viewed by those who need to know in order to carry out their duties in accordance with this procedure.

External Notifications

69. **Information Commissioner's Office (ICO)**. The DPO (or their nominee) will act as a point of contact between the ICO and the Council. Any incidents resulting in risk to data subjects may amount to a serious breach and require notification to the ICO. Such breaches should be notified to the ICO within 72 hours of the Council first becoming aware. Where information is not available at the time of reporting, it should be provided to the ICO as soon as it is available.

70. The Data Protection Officer (DPO) (or their nominee) will be responsible for notifying the ICO where the breach is assessed as being a risk to data subjects' rights and freedoms. The DPO will liaise with the ICT Security Team (if necessary) and will consult with the Senior Information Risk Owner (SIRO) and Caldicott Guardian (where appropriate) prior to any notification to the ICO or other parties.

71. **Data Subjects.** There is a requirement to communicate a personal data breach to data subjects where it is likely to result in a high risk to their rights and freedoms. This should be done as soon as possible after that risk assessment has been made. The data subject should be provided with:

    - the name and contact details of the Incident Lead, Data Protection Officer or another contact point where more information can be obtained;
    - the likely consequences of the personal data breach; and
    - a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

72. The Incident Lead will be responsible for ensuring the affected data subject(s) are notified, typically first verbally and then in writing. They need not do this themselves but it needs to be someone in the business who is able to assume

responsibility for the breach having occurred (typically this will be a Team, Service or Group Manager). Advice and letter templates will be made available by the assigned Incident Support Officer to support this task.

73. **Organisations for whom the Council processes data.** Where the incident involves data which the Council processes for third party organisations e.g. schools; Alternative Service Delivery Models such as Arc (Property), Inspire (Libraries) Via (Highways), the incident will require notification to that third party in accordance with the requirements of the Council's data processing agreement and / or contract with them. Where there is no such requirement, the organisation's Data Protection Officer (DPO) or a senior manager needs to be made aware. The NCC contract manager also needs to be made aware of the breach.

74. The Information Governance Team will provide advice on any other notifications as appropriate for affected stakeholders depending on the established facts of the incident.

Roles and Responsibilities

75. All staff including: employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information staff must be aware of and comply with this procedure.

76. Duties assigned to specific roles referenced in this procedure must be carried out as described. The Council's Information Governance Framework provides further detail of the nature of specific information governance related roles (e.g. that of SIRO, Caldicott Guardian, Data Protection Officer etc.).

77. HR will provide advice to parties implementing this procedure on any employment implications arising from security incidents or breaches.

78. The Council's Data Protection Officer and Information Governance Team must ensure that the requirements described in this procedure are implemented and maintained.

Compliance with this Procedure

79. The Data Protection Officer (or their nominee) may become involved in an incident at any stage if any stage of this Procedure is not progressing to a satisfactory outcome, and the matter may be escalated to SIRO / Caldicott Guardian.

80. The Council wishes to foster a culture in which security incidents and data protection breaches are reported. The key objective is to develop valuable insight into how such events occur and staff can be assured that reporting a breach will not in itself result in disciplinary action.

81. However, wilful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter under the relevant employment procedure(s) which could lead to dismissal or the termination of work agreement or service contracts.

82. Personal data breaches which are the result of an intentional action or inaction may give rise to criminal charges under the Data Protection Act and Computer Misuse Act.

Review

83. This procedure will be regularly monitored and reviewed by the Data Protection Officer (or their nominee) who will revise it in line with learning arising from the implementation of the procedure.

84. Beyond that, the procedure will be monitored and reviewed annually in line with legislation and codes of good practice.

Advice, Support & Further Information

85. If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact:

The Information Governance Team
Email: data.protection@nottscc.gov.uk
Telephone: 0115 8043800

86. Further reading and supporting information:

Title (as hypertext link) and publication date	Author
Guide to the Notification of Data Security and Protection Incidents (September 2018)	NHS digital
Personal data breaches (webpages as at November 2018)	ICO

--- ENDS ---

Version Control – Post Approval

V	Date	Author	Approved by	Comments
1.0	7/12/18	C Agnew	Info. Gov. Group	
1.1	9/1/19	C Agnew		To reflect HR comments (Gill Elder) and update

Appendix A – Incident Assessment Form

Nottinghamshire County Council

Data Incident & Breach Reporting Form

Note: This form is to be used when reporting a data / incident breach. Those completing the form should avoid referencing personal details (e.g. name of data subjects etc).

Contact & overview details					
NCC Ref No					
Reporter Name					
Job Title					
Email		**Tel No**			
Team					
Dept					
Did the person reporting the incident also discover it?			**Yes** ☐	**No** ☐	
If no	**Who did discover it?**				
	Reporter's relationship to discoverer?				
	Which team's data is affected?				
	The team is in which Dept?				
Who has been told about the incident?					
Team / Service Manager email:					
Group Manager email:					
Date Reported	Click here to enter a date.	**Time Reported**			
Information Governance Team Use					
Method of reporting:					
Phone report completed by:					
Have you obtained a copy of the material that created caused the breach?		**N/A** ☐	**Yes** ☐	**No** ☐	
Have you saved it in Respond?			**Yes** ☐	**No** ☐	

Incident details
Tell us as much as you can about the incident, what happened, what went wrong and how it happened?
How did you find out about the incident?

Date incident discovered?	Click here to enter a date.	**Time**	
Date incident happened?	Click here to enter a date.	**Time**	

If there has been any delay in reporting this incident, please explain why

Categories of personal data included in the incident (tick all that apply)?							
Data revealing racial or ethnic origin	☐	Health data	☐	Sex life data	☐	Sexual orientation data	☐
Gender reassignment data	☐	Political opinions	☐	Religious or philosophical beliefs	☐	Trade Union membership	☐
Criminal convictions offences	☐	Biometric or genetic data	☐	Location data	☐	Basic personal identifiers (e.g. name, contact details)	☐
Identification data (e.g. usernames, passwords)	☐	Official documents (e.g. drivers licences)	☐	Economic & financial data (e.g. credit card numbers, bank details)	☐	Not yet known	☐
Other (Give details)	☐						

Anything further re data sensitivity?	
Number of records involved in incident?	
How many data subjects could be affected?	

Categories of data subjects affected (tick all that apply)?					
Employees - NCC	☐	Employees of other organisations	☐	Contractors / advisors/consultants	☐
Suppliers	☐	Volunteers	☐	Students / pupils	☐
Service users – general	☐	Service users – children	☐	Service users – vulnerable adults	☐
Carers (& Reps)	☐	Suspected offenders	☐	Incident witnesses	☐
Complainants (& Reps)	☐	Holders of Public Office	☐	Not yet known	☐
Other (Give details)	☐				

From a business / professional perspective, What impact has the incident had/is likely to have on the affected individual(s)?

Reports of incidents from / regarding NCC's data processors (e.g. care homes, Inspire, Via etc)		
Did this incident originate at an NCC data processor?	**Yes** ☐	**No** ☐
If yes, give details of the organisation, whether there is a GDPR compliant contract in place with the organisation and the NCC contract manager?		

Initial Containment / Mitigation Actions		
Has any lost / disclosed data been recovered?	**Fully** ☐	**Partially** ☐
Describe the actions you have taken, or propose to take, as a result of the incident E.g. confirmed the extent of disclosure of data sent in error and that it has been recovered / destroyed, reviewing working practices and guiding change etc		

Third parties			
Was the data affected by the incident collected by NCC on behalf of and/or used to provide its services for other organisations (e.g. payroll for schools, pensions for borough councils etc)?	**Yes** ☐	**No** ☐	
If yes, please provide details of the organisations concerned and the nature of the services that NCC provides to them and any other material details?			
NCC contract manager name (if known)?			
Has the NCC contract manager been made aware of the incident?	**Yes** ☐	**No** ☐	
Has the organisation whose data has been affected be notified of the incident?	**Yes** ☐	**No** ☐	
If yes, incident notified?	Click here to enter a date.	Time	
Are there any other organisations that have been/should be made aware of this incident (e.g. the police where theft is involved, NHS where data that has been shared with NCC by Health Services has been affected etc)?			

Severity Assessment

This section is to be completed by the assigned Information Governance Advisor on the basis of details established in dialogue with the appropriate business lead [to reveal this section click small triangle to the left of the start of this paragraph]

Assessment of Severity - To be completed by the DPO (or nominee) in consultation with the Group Manager of area affected by the breach and others as appropriate.			
Is this a confirmed personal data breach?	**Not yet known** ☐	**Yes** ☐	**No** ☐
If no, is it a near miss?		**Yes** ☐	**No** ☐
Aspect(s) of security impacted	**Confidentiality** – accidental / unauthorised disclosure of, or access to, personal data		☐
	Integrity – accidental / unauthorised alteration to personal data		☐
	Availability – accidental / unauthorised loss of access to or destruction of personal data		☐

Section	Factor	Max Score	Score	Score Rationale / Comments (important for audit trail)
Scale: Number of people's data breached (Max 5)	0-10	**1**		
	11-100	**2**		
	101-1,000	**3**		
	1,001 or more	**5**		
Who was the data disclosed to?	Internal (same service)	**0**		
	Internal (different service)	**1**		
	External – another business, organisation, e.g. the NHS	**2**		
	External – a member of the public	**3**		
	External – multiple members of the public	**4**		
	External – unknown members of the public	**4**		

Types of Data (Max 7)	Simple (personal)	**1**		
	Special Category / sensitive	**2**		
	Personal Financial	**2**		
	Commercially Sensitive	**2**		
	Public	**0**		
Likelihood of data subjects suffering significant consequences as a result of incident? (Max 3)	Very unlikely	**0**		
	Unlikely	**0**		
	Neutral	**1**		
	Likely	**2**		
	Very likely	**3**		
	Not known (Explain)	**1**		
Risk Factors (Max 10)	Identification of data subject	**1**		
	High-risk confidential information	**3**		
	Physical harm – data subject	**2**		
	Damage or distress – data subject	**2**		
	Media attention to data subject	**2**		
Score				**Risk Rating**

Severity Scale by Score		**Notification Action Arising (scores act as a guide to external notification only)**
Very High	Score **=/>16**	Likely to require reporting to ICO and data subject(s). Notify the DPO immediately who liaise with the SIRO, / Caldicott Guardian (separate form required)
High	Score **12-15**	Likely to require reporting to ICO. Notify SIRO, Caldicott Guardian

Medium	Score **8-11**	Notify Caldicott Guardian
Low	Score =/**<7**	Notify Group Manager / DPO of all breaches

This severity assessment accurately reflects the signatory's understanding of the nature, context and severity of the security incident / breach.			
Comments:			
Name		**Date**	Click here to enter a date.

Incident Investigation

This section is to be completed by the incident investigator, who will ordinarily be the Team / Service Manager of the team within which the incident / breach occurred or someone appointed by either the Information Asset Manager (Group Manager) or Information Asset Owner (Service Director) to undertake the investigation.

For incidents / breaches with a severity assessment of Low, the assigned Information Governance Advisor will complete this section in dialogue with the appropriate business lead [to reveal this section click small triangle to the left of this paragraph]

CONTACT DETAILS			
Investigator Name			
Job Title			
Team			
Dept			
Email		**Tel No**	
IG Support Name			
Email		**Tel No**	
INCIDENT DETAILS			
Was the incident reported to the ICO as a personal data breach?	**Yes** ☐	**No** ☐	
If yes, please add ICO reference number			
Have the affected data subjects been made aware of the breach?	**Yes** ☐	**No** ☐	
Are copies of any correspondence with the data subject(s) available upon request?	**Yes** ☐	**No** ☐	
Have any other parties been made aware of the breach?	**Yes** ☐	**No** ☐	
If so, please provide details of the parties			

Are there any new findings about the incident / breach?	**Yes** ☐	**No** ☐
If yes, please specify (including the nature / extent of the data disclosed, the numbers of people the data was disclosed to, how it occurred etc)		
Was any lost / disclosed data retrieved and / or destroyed?	**Yes** ☐	**No** ☐
Please provide details to support answer given, including specifying the reason why the data was not retrieved and / or destroyed where that was a possibility.		
Were any additional containment / mitigation actions taken to reduce the impact of this incident / breach on affected individuals?		
Describe the measures that were in place before this breach occurred to prevent an incident of this nature occurring (e.g. procedures; training etc)		
What should have happened to prevent this incident occurring?		
Have any additional impacts on the affected individual(s) been identified?		
Currently, have any individuals complained about the breach / incident?	**Yes** ☐	**No** ☐
If yes, please provide details		

Had the staff member(s) responsible for the incident / breach completed the NCC's GDPR / info security training in the past two years?	**N/A** ☐	**Yes** ☐	**No** ☐
If yes, when and if not, why not?			
Please provide any other important comments about the data breach and its impact			
LEARNING FROM THE INCIDENT			
How can this type of data breach be prevented in the future?			

Would you recommend documenting and / or changing any processes to stop future occurrences of this incident / breach?	**Yes** ☐	**No** ☐
If yes, please provide details.		

What learning & actions will be taken to prevent this type of incident reoccurring within the Group / Team? For investigator in conjunction with Team / Group Manager.		
Learning and Resulting Action	**By Who**	**By When**
Example Staff not trained – ensure all staff trained annually	J Smith	31/12/18

Do you have any suggestions about how the corporate incident / breach procedure could be improved
Please provide any other final comments about the data breach and its impact

SIGN-OFF This investigation form accurately reflects the investigator's understanding of the incident / breach and the associated learning and actions needed to limit residual harm and prevent reoccurrence			
Comments:			
Name		**Date**	Click here to enter a date.

Incident Review

This section is to be completed by the assigned Information Governance Advisor [to reveal this section click small triangle to the left of this paragraph]

Learning from the Incident [to be completed by the assigned Information Governance Advisor]		
Are there any other learning & actions (in addition to that should be taken to prevent this type of incident reoccurring within the Group / Team)?	**Yes** ☐	**No** ☐
If yes, please provide details and ensure these are shared with the investigator for inclusion in their learning / actions section above.		
Are there any learning implications for the wider organisation?	**Yes** ☐	**No** ☐

Learning and Resulting Action	**By Who**	**By When**

Is there any learning & actions that could improve the corporate breach / incident procedure? (Include actions associated with suggestions made by the investigator)		
Learning and Resulting Action	**By Who**	**By When**
Any other comments on this investigation?		

Have there been any similar breaches in NCC in the past 2 years?	**Yes** ☐	**No** ☐
If yes, please provide details		
Has the team had any other breaches in the past 2 years?	**Yes** ☐	**No** ☐
If yes, please provide details (numbers, type etc)		

Sign-off

This investigation form accurately reflects the investigator's understanding of the incident / breach and the associated learning and actions needed to limit residual harm and prevent reoccurrence

Comments:

Name		**Date**	Click here to enter a date.

Appendix B - Incident Flowchart