Nottinghamshire County Council

Data Security Incident & Breach Management Procedure

At a glance …

- A data security incident / breach affects the confidentiality, integrity or availability of personal or confidential data (including destruction, loss, alteration, unauthorised disclosure or access) and must be reported immediately.
- Report incidents without delay, Line manager(s) should also be informed but this should not delay reporting.
- The Council may be required to report certain breaches to the Information Commissioner's Office (ICO) within 72 hours and to notify affected individuals where there is a high risk.
- The IG Team coordinates the incident and breach management [tel: 0115 8043800]. IT-related incidents must also be reported via the ICT Service Desk [tel: 0115 977 2010].
- Immediate action should be taken to contain and minimise impact (e.g. retrieve or secure data disclosed in error). Advice will be provided upon reporting.
- Where the Council processes data on behalf of, or shares data with, other organisations, relevant parties must be notified of breaches without delay.
- Organisations working for the Council must report breaches to us immediately and contract provisions must require this.
- All incidents are logged. More serious incidents will be investigated to identify causes, mitigate risks and prevent recurrence.
- Relevant senior officers (including Heads of Service / Group Managers, the Data Protection Officer (DPO), SIRO and Caldicott Guardian, as appropriate) will be informed based on severity.
- The DPO will determine, in consultation with relevant roles, whether notification to the ICO and/or data subjects is required.
- Data breach reports will be produced to support organisational learning and improvement.
- Individuals have the right to raise a data protection complaint, including where they believe a personal data breach has occurred. Such allegations will be recorded and, where appropriate, investigated in line with this procedure and the Data Protection Complaints Procedure.
- Individuals may request an internal review of the Council's response to a reported data breach, subject to defined criteria and timescales.

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 data 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 and complements the ICT Cyber Security Response Process.

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. Data security incidents are dealt with quickly and efficiently.
    b. A consistent approach is applied to management and reporting of data security incidents
    c. The damage caused by data security incidents is minimised.
    d. The likelihood of a recurrence of a data 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. Reference to information and data 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 information or data 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 deemed to the case the breach must be reported within 72 hours (including weekends) 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 29.

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. 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.

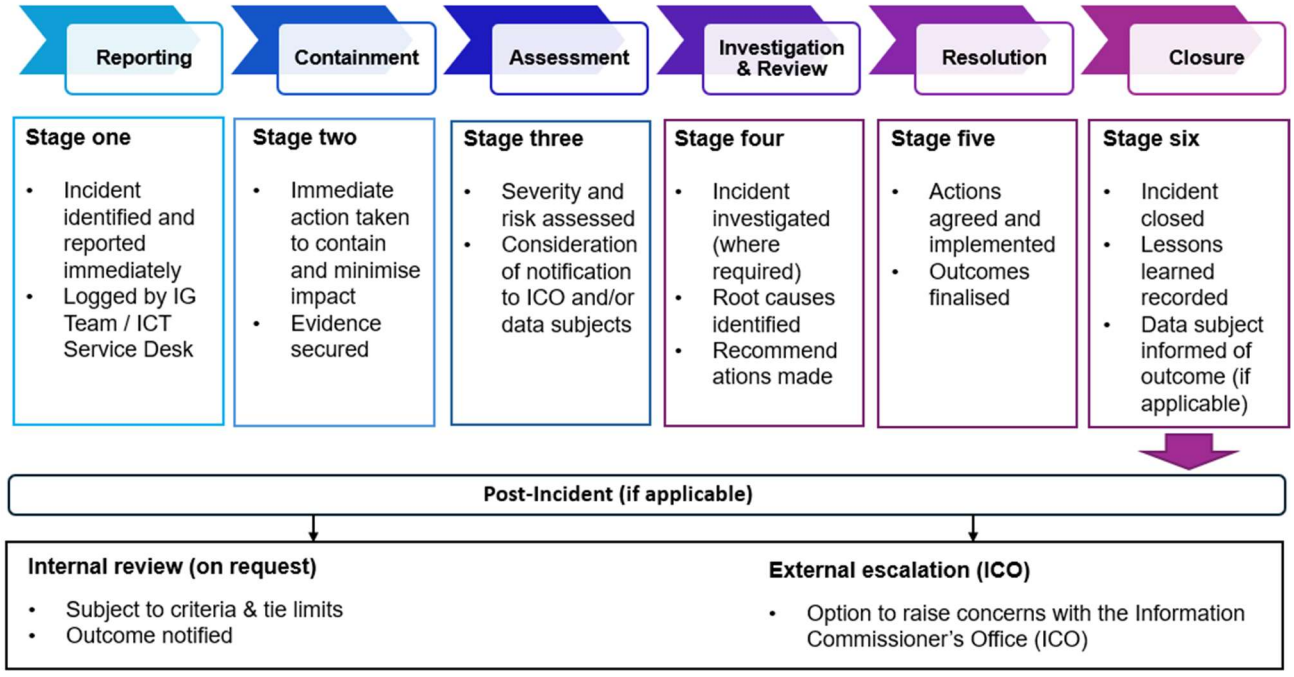
22. The principles of this procedure also apply to cyber incidents. Cyber incidents are any incidents that could or have compromised information assets within the Council's digital network (e.g. phishing emails or hacking attacks). Any cyber-related incident will be handled in accordance with the Council's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

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.

24. The Council recognises the right of individuals to raise a data protection complaint, including where they believe their personal data has been subject to a breach, in accordance with applicable data protection legislation (including the Data (Use and Access) Act). Any such complaints will be handled in accordance with the Council's Data Protection Complaints Procedure and, where relevant, this Data Security Incident & Breach Management Procedure.

Incident Management

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



Stage 1 – Incident Reporting

26. 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.

27. 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.

28. 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.

29. 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 • 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	**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 • 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

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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).

36. Where an individual (or their representative) contacts the Council alleging that a personal data breach has occurred, this will be recorded as a data protection complaint. The matter will be assessed and handled in accordance with both this Procedure and the Data Protection Complaints Procedure. Where appropriate, it will also be logged and managed as a data security incident to ensure investigation, risk assessment and regulatory reporting requirements are met.

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

<u>Stage 2 – Incident Containment</u>

38. The line manager of the member of staff who has committed a data breach is responsible for ensuring actions are carried out where appropriate, to prevent further disclosure or damage as soon as practical.

39. 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.

40. 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

41. The severity of an incident will be determined by a data incident assessment for which there will be an Incident Severity Assessment Form (available from the Information Governance Team).

42. 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.

43. Allegations of data breaches raised by data subjects will initially be treated as complaints and assessed to determine whether there is sufficient evidence of an information security incident. Where an allegation is substantiated, it will be notified internally, formally recorded as a data security incident and progressed through the incident management process, alongside the complaints handling process.

44. 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.

45. 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 / or Caldicott Guardian (or their deputies), where appropriate.

46. 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.

47. Depending on the nature of the data incident, it may be appropriate to notify affected data subjects regardless of the initial risk assessment rating. The Data

Protection Officer (or their nominee) will make an appropriate recommendation in such cases.

Stage 4 – Incident Investigation & Review

48. 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.

49. 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.

50. Where the incident is assessed as being of medium or higher severity, the Group Manager / Head of Service of the team in which it occurred will appoint an Incident Lead to investigate the incident where this is recommended by the Information Governance Team. For all other incidents, the line manager of the person responsible for the incident will carry out the investigation where necessary.

51. 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.

52. 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.

53. 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.

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

55. 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.

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

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

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

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

60. 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.

61. Where a data protection complaint has been made in relation to the incident, the investigation carried out under this procedure will inform the Council's response to that complaint. Coordination between the incident investigation and the complaints process will ensure a consistent, accurate and timely response to the data subject.

Stage 5 – Incident Resolution

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

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

Stage 6 – Incident Closure

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

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

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

67. The DPO (or their nominee) will report incident performance to the Information Governance and Cyber Security Board on a quarterly basis and to any appropriate departmental groups as and when required. This will contain both quantitative and qualitative data, providing analysis on incident trends, incident management and incident lessons learned / to be learned.

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

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

70. Following closure of an incident, where a data subject has raised a complaint or allegation of a personal data breach, they will be informed of the outcome and of their right to request an internal review of the Council's response, subject to defined criteria and timeframes.

Data Subject Complaints and Post-Incident Review

71. This stage forms part of the overall lifecycle of managing a reported personal data breach, providing individuals with the opportunity to seek review of the Council's response once the incident investigation and response have been completed.

72. Following the Council's response to a reported personal data breach, an individual may request an internal review of that response. The opportunity to request a review will be outlined in the Council's initial response.

73. Any request for an internal review must be made within a reasonable timeframe (no later than 30 days after receiving the initial response to the breach complaint) and must clearly set out the grounds on which the review is sought. Reviews will only be undertaken on defined grounds, namely that the Council:

    a) failed to follow applicable data protection legislation;
    b) did not adhere to its own breach response procedures;
    c) made a material error in interpreting the facts available at the time; or
    d) otherwise acted unreasonably considering the information then known.

74. The purpose of an internal review is to assess whether the original breach response was handled appropriately, based on the information and circumstances known at that time. Any new matters, evidence, or concerns raised after the initial response fall outside the scope of the internal review process and must be pursued separately through the appropriate channels. The outcome of the internal review will confirm whether the original response is upheld or identify any procedural or decision-making issues.

75. Data subjects retain the right at any stage to raise their concerns directly with the Information Commissioner's Office (ICO), irrespective of whether they have requested or completed the Council's internal review process. However, the ICO will ordinarily expect individuals to have first given the Council a reasonable opportunity to consider and resolve the matter before referring it for external consideration.

76. Internal reviews of data breach decisions will be undertaken by Senior Information Governance Advisors (SIGAs) within the Information Governance (IG) team who have had no prior involvement in the handling of the original breach response or outcome.

77. The review will be carried out as promptly as practicable, ensuring a fair and independent reassessment of the case. A written response will be provided to the requester, setting out the findings of the internal review and the rationale for the decision. The response will also inform the requester of their right to escalate the matter to the Information Commissioner's Office (ICO) should they remain dissatisfied with the outcome.

Notification of incidents

Internal Notifications

78. Internal notifications will be determined in accordance with the incident rating as set out in Incident Assessment Form. The IT Service Desk or IG Team will be responsible for notifications as appropriate.

79. The relevant Group Manager / Head of Service will be notified of all incidents that have occurred solely within their areas of responsibility, the Service Director will be notified where the severity rating is medium or above. They will be required to nominate an Incident Lead to investigate the more serious incidents (i.e. those assessed as medium severity or above as recommended by the IG Team).

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

81. 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

82. **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.

83. 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.

84. **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.

85. 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.

86. Data subjects will also be informed of their right to raise a data protection complaint with the Council and, where applicable, with the Information Commissioner's Office (ICO). Information on how to do so will be provided in line with the Council's Data Protection Complaints Procedure.

87. **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.

88. **Department for Work and Pensions.** Any actual or suspected incidents involving DWP, HMRC or Home Office derived data, including suspected misuse (clerical or electronic) or ICT network issues that could compromise

such data, will be reported to lawelfare.lasecurity@dwp.gov.uk. The Incident Lead (or their nominee) is responsible for ensuring that such reports are made promptly and in accordance with relevant agreements and protocols. Advice will be provided by the assigned Incident Support Officer.

89. 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

90. 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.

91. 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.) see also the intranet page on IG roles and responsibilities.

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

93. 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

94. 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 the SIRO / Caldicott Guardian.

95. 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.

96. 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.

97. 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

98. 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.

99. Beyond that, the procedure will be monitored and reviewed every three years in line with legislation and codes of good practice.

Advice, Support & Further Information

100. 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

Document Control

Owner	Data Protection Officer
Author	Caroline Agnew, Data Protection Officer
Last Reviewer	Caroline Agnew, Temporary IG Programme Advisor
Approver	Data Protection Officer
Date of Approval	30/06/2026
Date of next review	29/06/2029
Version	1.4
Classification	Public

Version	Date	Changes and Approver
1.0	07/12/2018	Original document approved by Information Governance Group
1.1	02/08/2019	Changes to reflect HR and Health and Safety comments and to update some aspects of process.
1.2	21/06/2022	(JM) General review and updates to incident investigation requirements
1.3	30/09/2025	(JM) General review and updates to incorporate DWP reporting requirements
1.4	30/06/2026	Updated to incorporate data protection complaint handling, introduction of internal review process, and revision of incident management schematic, flow chart and supporting text

Appendix A - Incident Flowchart