Draft Code of data matching practice 2026

Issued under Section 26F of the Public Finance and Accountability (Scotland) Act 2000

AUDIT SCOTLAND

Prepared by Audit Scotland
July 2026

Contents

Accessibility

You can find out more and read this report using assistive technology on our website www.audit.scot/accessibility.

Foreword

Audit Scotland is committed to ensuring that public money is spent well to meet the needs of Scotland's people. In Public audit in Scotland 2023–28 we set out this vision alongside our mission to provide clear, independent and objective assurance on how effectively public money is being managed and spent. The National Fraud Initiative (NFI) in Scotland is one of the ways that we do this, helping to ensure that public bodies work better together to target resources and make financial management more effective.

The NFI is a counter-fraud data matching exercise across the UK public sector. The Cabinet Office oversees the NFI and Audit Scotland leads the exercise in Scotland. It remains a very successful example of efficient joined-up working among public bodies to secure improved financial controls and measurable savings.

Audit Scotland has explicit powers under the Public Finance and Accountability (Scotland) Act 2000 and Section 97 of the Criminal Justice and Licensing (Scotland) Act 2010 to undertake data matching exercises. Importantly, the legislation includes safeguards for those individuals whose data is submitted for data matching. These include a requirement for Audit Scotland to prepare and keep under review a Code of Data Matching Practice (the Code), after consulting bodies that participate in the NFI and the Information Commissioner's Office.

The Code sets out the principles and practices that should be adopted by those taking part in the NFI and other data matching exercises undertaken by Audit Scotland. Key aspects of the Code include examples of how individuals should be informed that their personal information will be used for data matching and how data will be submitted by, and returned to, participating bodies using a secure online system.

Audit Scotland is grateful to the respondents to our consultation on this Code and for their helpful comments. In particular, we are appreciative of the advice from the Information Commissioner's Office on the Code.

The Code comes into immediate effect and applies to Audit Scotland, the Cabinet Office which processes data on our behalf, participating bodies in Scotland and the appointed external auditors who monitor their participation.

Stephen Boyle
Auditor General for Scotland and
Accountable Officer for Audit Scotland

1. Introduction to the Code

The Code of data matching practice

1. In our audit work, under the Code of audit practice, we consider fraud risks. As part of this consideration, we may look at data that is held by different public bodies and compare these data sets to see if there are any trends or patterns that may indicate fraud and need to be investigated. This is called data matching. Handling and managing data about individuals needs to be done securely and sensitively. We have prepared this Code of data matching practice to help make sure that Audit Scotland and its staff, auditors and all persons and bodies involved in **data matching exercises**[1] comply with the law, especially **data protection legislation**.

2. This Code creates a balance between preventing and detecting fraud, and the importance of paying due regard to the rights of those people whose data are matched for this purpose. It aims to promote good practice in data matching and will provide a robust framework for the future development of Audit Scotland's data matching activities.

3. The previous version of the Code was published in 2018. The 2026 Code has been reviewed and refreshed to:

- make reference to The Digital Government (Scottish Bodies) Regulations 2022 and clarify the UK GDPR principles that apply
- include details of the use of NFI data in private sector fraud detection and prevention services
- ensure consistency with current data protection legislation applicable in the UK, including amendments made by the Data (Use and Access) Act 2025.

4. The Data (Use and Access) Act 2025 does not replace the UK General Data Protection Regulation or the Data Protection Act 2018 but makes targeted amendments to them. These amendments do not change the statutory basis on which Audit Scotland conducts data matching but are relevant to how participants understand and apply certain data protection requirements.

[1] Terms in bold are defined in the Appendix.

5. Separate investigatory and recovery powers conferred on public authorities by other legislation do not affect the audit-led data matching functions exercised by Audit Scotland under the Public Finance and Accountability (Scotland) Act 2000.

6. Audit Scotland recognises that data matching techniques and technologies will continue to evolve. Regardless of the tools or methods used, all data matching exercises must comply with the statutory framework, data protection legislation, and the principles set out in this Code.

The Auditor General for Scotland

7. The Public Finance and Accountability (Scotland) Act 2000 requires the AGS to appoint auditors to each **audited body** outside the local government sector in Scotland, including NHS bodies, colleges, Scottish Water, the police and fire services, the Scottish Government, government agencies and non-departmental public bodies in Scotland.

8. The AGS is the Accountable Officer for Audit Scotland.

The Accounts Commission

9. The Local Government (Scotland) Act 1973 requires the Accounts Commission to appoint auditors to each local government audited body in Scotland.

Audit Scotland

10. Audit Scotland is a statutory body set up under Section 10 of the Public Finance and Accountability (Scotland) Act 2000 to provide assistance and support to the AGS and the Accounts Commission. Audit Scotland employs the staff (including auditors) and incurs the expenditure (including the fees charged by firms appointed as auditors) required to support the functions of the AGS and the Accounts Commission.

11. Section 26A of the Public Finance and Accountability (Scotland) Act 2000 provides that Audit Scotland may carry out **data matching exercises** or arrange for them to be carried out on its behalf. In practice, most of Audit Scotland's data matching will be done as part of joint exercises such as the National Fraud Initiative (NFI). The NFI exercise is undertaken with the Cabinet Office and the other UK public sector audit agencies. The key aspects of these exercises, such as the collection and processing of data, will usually be undertaken by the Cabinet Office and any firm with which it is contracted, on behalf of Audit Scotland and the other audit agencies.

Background to the National Fraud Initiative

12. It is essential that public bodies have adequate controls in place to prevent and detect fraud. Fraud in central government, local government,

the health service and other public bodies is a major concern of those bodies as well as of Audit Scotland and those appointed by the AGS or the Accounts Commission to audit those bodies.

13. Data matching in the NFI involves comparing sets of data, such as the payroll or benefits records of a body, against other records held by the same or another body to see how far they match. The NFI will aim to avoid processing large amounts of personal data where there is not a significant risk of fraud being present. However, to allow potentially fraudulent claims and payments to be identified, it is necessary for the personal data of honest individuals to be processed as well.

14. Where no match is found, the data matching process has no material impact on those concerned. Where a match is found it indicates that there may be an inconsistency that requires further investigation. In the NFI, participating bodies receive a report of matches that they should follow up and investigate where appropriate. This enables them to detect instances of fraud, over or underpayments and to take remedial action and to update their records accordingly.

15. The NFI data matching currently comprises of two main strands. These are **batch matching** different sets of data and **point of application** matching (undertaken at the time a person applies for a benefit or service) for the purpose of prevention and detection of fraud.

16. Point of application matching is extended to public and private sector participants and the Cabinet Office also provides search access the NFI data pool to private sector companies for use in their own counter fraud products and services. These products and services are for approved purposes with the focus on point of application checks and checking of existing caseload to identify and prevent fraud.

The statutory framework

17. Audit Scotland conducts **data matching exercises** under statutory powers added to the Public Finance and Accountability (Scotland) Act 2000 by Section 97 of the Criminal Justice and Licensing (Scotland) Act 2010. Under the legislation:

- Audit Scotland may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud or other crime and in the apprehension and prosecution of offenders (referred to hereafter as the ‘permitted purposes’).
- Audit Scotland may require specified persons to provide data for data matching exercises. These include all the bodies to which the AGS or the Accounts Commission appoints auditors, licensing boards, and officers, office holders and members of these bodies or boards.

- Other persons or bodies may participate in Audit Scotland's data matching exercises on a voluntary basis. Where they do so, the statute states that there is no breach of confidentiality and generally removes other restrictions in providing the data to Audit Scotland.
- The requirements of data protection legislation apply.
- Audit Scotland may disclose the results of data matching exercises where this assists the purpose of the matching (see first bullet), including disclosure to bodies that have provided the data and to the auditors appointed by the AGS and the Accounts Commission.
- Audit Scotland may disclose both data provided for data matching and the results of data matching to the AGS, the Accounts Commission, the Cabinet Office, or any of the other UK public sector audit agencies specified in Section 26D of the Public Finance and Accountability (Scotland) Act 2000, where necessary for the purposes described in the first bullet.
- Wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence.
- Audit Scotland may impose reasonable charges on any body participating in a data matching exercise.
- Audit Scotland must prepare and publish a Code of Practice with respect to data matching exercises. All bodies conducting or participating in its data matching exercises, including Audit Scotland itself, must have regard to this Code.
- Audit Scotland may report publicly on its data matching activities.

18. The Digital Government (Scottish Bodies) Regulations 2022 allow Audit Scotland to receive information from HM Revenue and Customs data for Scottish residents.

Relationship to data protection legislation and other information sharing codes

19. In addition to this Code, when participating in data matching exercises, bodies should have regard to any other current data or information sharing codes and guidance, including any statutory guidance from the Information Commissioner which is available on the Information Commissioner's website.

20. References to compliance with data protection legislation should be construed as compliance with data protection legislation applicable in the UK, as defined in Section 3(9) of the Data Protection Act 2018, which includes the General Data Protection Regulation (EU) 2016/679 (UK GDPR) as amended by the Data (Use and Access) Act 2025.

21. HMRC share information using powers under the Digital Economy Act 2017 and the principles of the Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017 apply.

Structure of the Code

22. The order in which the Code is set out reflects the chronological stages of a data matching exercise. This is designed to make it easier for participating bodies to follow.

Review of the Code

23. Audit Scotland is required to keep the Code under review. It intends to update the Code in the light of changes in the law and to reflect comments and experience drawn from each **data matching exercise**.

Reproducing the Code

24. Bodies participating in data matching exercises may reproduce the text of this Code as necessary to ensure that all those involved are aware of their obligations in law and under this Code.

Queries on the Code

25. Any questions about this Code or a particular data matching exercise should be addressed to Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN. Telephone: 0131 625 1500. Email enquiries should be addressed to: info@audit.scot and quote 'National Fraud Initiative' in the subject line.

Complaints

26. Complaints about bodies that are participating in Audit Scotland's data matching exercises should be addressed to the bodies themselves.

27. Complaints about Audit Scotland's role in conducting data matching exercises will be dealt with under its complaints procedure. Please contact Audit Scotland on 0131 625 1500 or email us at: complaints@audit.scot. Our complaints procedure is on our website.

28. A formal complaint should be made on the complaints form, which may be downloaded from the same web page and posted or emailed back to Audit Scotland. If you would like assistance in completing the form, please let us know.

29. Any concerns about the way that the NFI deals with personal data should be made to the Information Commissioner.

2. The Code of data matching practice

Status, scope and purpose

30. Audit Scotland has drawn up this Code following a consultation process, as required by Section 26F of the Public Finance and Accountability (Scotland) Act 2000. It replaces the Code published in November 2018 and applies from the publication date until such time as a replacement Code is prepared.

31. This Code applies to all **data matching exercises** conducted, by or on behalf of, Audit Scotland under Part 2A of the Public Finance and Accountability (Scotland) Act 2000 for the purpose of:

- assisting in the prevention and detection of fraud
- assisting in the prevention and detection of crime (other than fraud)
- assisting in the apprehension and prosecution of offenders.

32. Any person or body conducting or participating in Audit Scotland's data matching exercises must, by law, have regard to the provisions of this Code.

33. The purpose of this Code is to explain the data matching work the NFI does and to give guidance to Audit Scotland and its staff, auditors and all persons and bodies involved in data matching exercises on the law, especially the provisions of **data protection legislation**. The Code also aims to promote good practice in data matching. It includes guidance on the notification process for letting individuals know why their data is matched and by whom, the standards that apply and where to find further information. However, it is incumbent on all **participants** of the NFI to ensure their own procedures, when participating, are compliant with the law (including data protection legislation) as amended from time to time.

34. This Code does not apply to the detailed steps that should be taken by a participant to investigate matches from a data matching exercise. It is for participants to investigate matches in accordance with their usual practices for investigation of fraud etc.

35. The Information Commissioner regards the provisions of this Code as demonstrating a commitment to good practice standards that will help organisations to comply with data protection legislation.

What is data matching?

36. The Public Finance and Accountability (Scotland) Act 2000 and complementary legislation applying to other UK public sector audit agencies defines data matching as the comparison of sets of data to determine how far they match. In the Act, the purpose of data matching is to identify potential inconsistencies that may indicate fraud or assist with the other permitted purposes.

37. Where a match is found it indicates that there may be an inconsistency or circumstance that requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out by the **participant**.

38. The data compared are usually personal data. Personal data may only be obtained and processed in accordance with **data protection legislation**.

Who will be participating?

39. Under the Public Finance and Accountability (Scotland) Act 2000, Audit Scotland may require all audited bodies in Scotland, and other specified persons, to provide data for **data matching exercises**. This includes all the bodies to which the AGS or the Accounts Commission appoint auditors. Bodies required to participate in this way are referred to in this Code as **mandatory participants**.

40. Where it considers it appropriate, Audit Scotland may also accept data from **voluntary participants** in Scotland – ie, bodies that are not **mandatory participants**.

41. A range of public bodies in England, Wales, and Northern Ireland also participate in the NFI on a mandated and voluntary basis. Additionally, the Cabinet Office may include private sector organisations as participants in the exercise on a voluntary basis.

42. A small number of companies have also been granted limited search access to the NFI data pool for them to use in their anti-fraud data matching services. These organisations, identified in our NFI privacy notice, may search NFI data through secure systems using tiered levels of access, depending on the purpose of the request. This may include:

- Indicators only (eg, flags or match counts, without personal data).
- Redacted outputs, showing the nature of a match without identifying details.
- Core personal data, such as name, date of birth, National Insurance number and address.

- Enhanced data fields, which may include contextual information such as dates, or financial or benefit-related information.

43. Only agreed NFI datasets collected within the NFI are made available in this way, and access is controlled and proportionate to the purpose. These organisations configure how NFI-derived insights are used within their systems and may incorporate them into wider fraud prevention tools used by their clients. Where this occurs, these organisations are required to comply with the Cabinet Office Code of data matching practice and all aspects of UK GDPR.

Governance arrangements

Nominated officers

44. The Director of Finance or equivalent senior named officer of each **participant** should act as **senior responsible officer** for the purposes of **data matching exercises**.

45. The **senior responsible officer** should nominate officers responsible for data handling, for follow-up investigations and to act as a **key contact** with Audit Scotland and auditors, and should ensure that they are suitably qualified and trained for their role.

46. **Participants'** data protection officers should be involved at an early stage in the arrangements for data handling, training and providing privacy notices.

47. Audit Scotland's Chief Operating Officer has overall responsibility for data matching exercises and can be contacted at: Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN. Telephone: 0131 625 1500 or by email at: info@audit.scot quoting 'National Fraud Initiative' in the subject line.

48. Audit Scotland's NFI manager leads the day-to-day coordination of data matching exercises. They liaise with the Head of NFI and the NFI team at the Cabinet Office, who are responsible for matching data on Audit Scotland's behalf.

Audit Scotland guidance

49. For each data matching exercise, Audit Scotland will issue instructions and guidance to all participants. This will reference relevant Cabinet Office guidance and set out Scotland specific requirements. The most up-to-date instructions can be found on Audit Scotland's website.

Secure NFI website

50. The Cabinet Office has made available to Audit Scotland and **participants** a secure, password protected and encrypted website for **data matching exercises**, known as the secure NFI website. This site

allows participants to transmit data securely to Audit Scotland (in practice to the Cabinet Office which matches the data on behalf of Audit Scotland) and for the results of data matching to be made available in secure conditions. Participants also have access to further Cabinet Office guidance material and training modules on this website, including reports on the quality of their data and information on how to interpret matches, and on co-operation between participants.

How Audit Scotland chooses data to be matched

51. Audit Scotland will only choose data sets to be matched where it has reasonable evidence that one of the data matching purposes permitted by the Public Finance and Accountability (Scotland) Act 2000 or of the Criminal Justice and Licensing (Scotland) Act 2010 will be met as a result of matching those data sets. This will be a key consideration when Audit Scotland decides whether it is appropriate to accept data from a **voluntary participant**, or to require data from a **mandatory participant**. Evidence may come from previous **data matching exercises**, pilot exercises, from participants themselves or from other reliable sources of information such as auditors and the police.

52. Audit Scotland will undertake new areas of data matching on a pilot basis to test their effectiveness in serving the permitted purposes. Only where pilots achieve matches that demonstrate a significant level of success (eg, potential fraud) should they be extended nationally. A small number of serious incidents of fraud or a larger number of less serious ones may both be treated as significant. The terms of this Code apply in full to pilot exercises. Pilot data must be provided in accordance with the provisions of **data protection legislation**.

53. Audit Scotland may also undertake data matching based on the results of previous data matching exercises or pilot exercises that have been undertaken by the Cabinet Office or one of the other UK public sector audit agencies.

54. Audit Scotland (or the Cabinet Office) will review the results of each exercise in order to refine how it chooses the data for future exercises.

The data to be provided

55. The data required from participants will be the data that is adequate, relevant and limited to what is necessary to undertake the matching exercise, to enable individuals to be identified accurately and to report results of sufficient quality. This will be set out in the form of a data specification for each data set in the instructions for each exercise.

56. In Scotland, National Insurance numbers are not required in the data specifications for electoral roll, creditor and council tax data submissions. Other data specifications request National Insurance numbers to help improve accuracy of data matches.

57. The senior responsible officer at each participant will normally be notified about any revisions to the data specifications at least six months before the data is to be provided. This is to ensure that participants have early notification of any changes, so they can prepare adequately.

Powers to obtain and provide the data

58. All **mandatory participants** must provide data for data matching exercises as required by Audit Scotland under Section 26C (1) of the Public Finance and Accountability (Scotland) Act 2000. Failure to provide data without reasonable excuse is a criminal offence under Section 26C (5) of the Act.

59. The provision of data to Audit Scotland by a voluntary participant does not amount to a breach of confidentiality and generally does not breach other legal restrictions. This is provided for in Section 26B of the Public Finance and Accountability (Scotland) Act 2000. The provision of data to Audit Scotland for data matching by a **voluntary participating body** must comply with **data protection legislation**.

60. **Patient data** may not be shared voluntarily, and so may only be used in data matching if Audit Scotland requires it from a mandatory participant.

61. Whether participants provide data on a mandatory or voluntary basis, they are still required to provide the data in accordance with the provisions of data protection legislation.

62. In most cases, data matching will take place in accordance with the data protection principles with no need to rely on exemptions.

63. Voluntary Participants must have undertaken a data protection impact assessment (DPIA) in advance of submitting datasets for matching.

64. The processing of personal information under the NFI is lawful on the basis of the principles within UK GDPR Article 6 and DPIAs should typically cite the public task or legitimate interest principles, including recognised legitimate interests introduced by the Data (Use and Access) Act 2025. Guidance on lawfulness principles can be found on the Information Commissioner's Office website.

65. The processing of data by Audit Scotland in a data matching exercise is lawful and carried out with statutory authority. It does not therefore require the consent of the individuals concerned.

Fairness, privacy and transparency

66. **Data controllers** must process data lawfully, fairly, in a transparent manner and for specified and legitimate purposes. In addition, data controllers must inform individuals that their data will be processed. Participating bodies must therefore provide a written notice, known as a privacy notice, which contains the information required by **data protection**

legislation. Guidance is available from the Information Commissioner's Office website.

67. Audit Scotland issues an overarching NFI privacy notice as data controller for the exercise in Scotland. As part of a layered approach to privacy notices, participating bodies may wish to link to this overarching privacy within their own notices.

Privacy notices

68. The privacy notice should contain information required by data protection legislation such as:

- the identity of the data controller
- the purpose or purposes for which the data may be processed
- the legal basis which the controller is relying on for processing
- the categories of personal data collected
- the recipient or category of recipients of personal data
- details of retention period or criteria on retention
- the source of the personal data
- the right to lodge a complaint with the Information Commissioner, and
- any further information that is necessary to enable the processing to be fair.

69. **Participants** should, so far as practicable, ensure that privacy notices are actively provided to the individuals about whom they are sharing information. The notice should clearly set out an explanation that their data may be disclosed for the purpose of preventing and detecting fraud (or other permitted purpose, as appropriate) and include details of the legal basis on which the data controller relies for the processing. The notice should state that the data will be provided to Audit Scotland for this purpose and it should also specify who the data will be shared with. The notice should also contain details of how individuals can find out more information about the processing in question.

70. Communication with individuals whose data is to be matched should be clear, prominent and timely. Where data matching is being undertaken at the **point of application**, then the notification provided at this time would suffice. It is good practice for reminder notices to be issued before each round of **data matching exercises**. The Information Commissioner's guidance mentioned above advises on when you should actively communicate privacy information.

71. When providing data to Audit Scotland, **participants** should submit a declaration, using the facility available on the NFI secure website, confirming compliance with the privacy notification requirements. If Audit Scotland or an auditor becomes aware that privacy requirements have not been adhered to, they should agree the steps necessary for the participant to achieve compliance. Audit Scotland may seek input from the Information Commissioner as part of this process.

Collection of new data

72. Participants should provide privacy notices at the point of collecting personal data where practicable. It is for participants to ensure privacy notices are in line with **data protection legislation**, as it stands at the time; and in line with the current Information Commissioner's guidance, that they provide the appropriate form of notice at the appropriate time to meet the requirements of fairness and transparency. Participants should in any event provide such notices before disclosure of the data to Audit Scotland, unless it is impracticable to do so.

Deceased persons

73. Some of the data used for data matching exercises relates to deceased persons. Although information relating to a deceased individual cannot be regarded as personal data of the deceased person under the data protection legislation, common law rules of confidentiality may restrict disclosure in certain circumstances. In order not to cause unnecessary distress or harm, particular care and sensitivity should be taken in dealing with data concerning deceased persons throughout the exercise, but particularly when investigating matches.

Quality of the data

74. Participants should ensure that the data they provide for data matching is of good quality (ie, accurate and complete) in line with data protection legislation, which requires personal information to be accurate and where necessary kept up to date. Processing of inaccurate and incomplete data could mean that the participant is in breach of data protection legislation.

75. Before providing data for matching, participants should ensure that errors identified from previous data matching exercises have been rectified, and action taken to address any issues identified in data quality reports supplied to the participant on the secure NFI website.

76. Linked to the requirement for data to be accurate is the right for data subjects to have inaccurate personal data rectified. Please refer to the Information Commissioner's guidance.

77. In addition to the right for data subjects to have inaccurate personal data rectified, data subjects also have the right to have personal data

erased or restricted. If a data subject exercises any of these three rights with a **participant** and the participant is required to comply with such rights in accordance with **data protection legislation**, then the participant must also communicate this to Audit Scotland as a recipient of the personal data, However, if an exemption under the Data Protection Act 2018 applies, then the participant may not have to comply with the request to exercise the right. Participants should always consider whether it has provided Audit Scotland with accurate personal data.

Security

78. Audit Scotland, the Cabinet Office and any firm undertaking matching as its agent, and all participants must put in place security arrangements for handling and storing data in **data matching exercises**. Such arrangements are to be of a technical and organisational security standard at least equivalent to ISO 27001.

79. These arrangements should ensure that:

- specific responsibilities for security of data have been allocated to one or more managers
- security measures take appropriate account of the physical environment in which data is held, including the security of premises and storage facilities
- there are physical and logical controls to restrict access to data held electronically, so that only those named individuals who need to access the data for the purpose of data matching exercises can do so
- all staff with access to data are given training that is sufficient to enable them to appreciate why and how they need to protect the data. Participants should refer to the training modules on the secure NFI website
- there are robust mechanisms in place for recording access, use and transfer of data
- if a breach of security occurs, or is suspected, authorised users are given new passwords or are required to change their passwords as soon as possible. The body responsible should consider what further steps it should take in the light of the Information Commissioner's guidance on management of security breaches.

80. Appropriate audit trails should be maintained to evidence that such arrangements are being complied with.

81. Transport Layer Security (TLS) is an encryption protocol used to protect data that is sent between computers. When two computers send data, they agree to encrypt the information in a way they both understand.

Depending on the rules in place, either of them may refuse to connect if they can't find a suitable encryption method.

82. In August 2018, the NFI changed the level of TLS encryption to enable a more secure transfer when uploading data to the web application.

83. All persons handling data as part of the **data matching exercise** should be made aware of their data protection, confidentiality and security obligations under **data protection legislation** and undertake training in this respect. Such staff should be subject to strict access authorisation procedures. Breach of authorisation procedures should attract appropriate disciplinary sanctions.

84. The NFI system goes through the Cabinet Office's information assurance and risk management process. The outcome of this is that the system is HM Government-accredited annually to store and process data.

85. Any firm processing data for the Cabinet Office will do so under a contract in writing that imposes requirements as to technical and organisational security standards, and under which the firm may only act on instructions from the Cabinet Office. The Cabinet Office, assisted by Audit Scotland and the other UK public sector audit agencies, will monitor the firm's compliance with these standards from time to time. In addition, the Cabinet Office requires annual security testing, supplemented by additional tests as appropriate.

86. Where the Cabinet Office undertakes data matching exercises on behalf of Audit Scotland or any other UK public sector audit agency there will be a similar written agreement in place.

87. Data protection legislation includes requirements, in certain circumstances, to report personal data breaches to the Information Commissioner within 72 hours, where feasible. There is also a requirement to notify the data subject of data breaches in certain circumstances (dependent on the nature of the data and an assessment of the potential risk to data subjects). For further guidance on security please refer to guidance, as updated from time to time, on the Information Commissioner's site.

Supply of data to Audit Scotland

88. Participants must only submit data to Audit Scotland via the Cabinet Office's secure NFI website or using an authorised **Application Programming Interface (API)**.

The matching of data by Audit Scotland

89. Audit Scotland will ensure that it matches data lawfully and fairly and for a purpose permitted by the Public Finance and Accountability (Scotland) Act 2000, eg assisting in the prevention and detection of fraud or other permitted purpose.

90. The Cabinet Office undertake the processing of data on behalf of Audit Scotland and apply data matching rules and predictive analysis techniques which seek to identify anomalies and potential inconsistencies for further investigation by participants and does not, in itself, result in decisions with legal or similarly significant effects being taken solely by automated means.

91. All data stored electronically by Audit Scotland, or the Cabinet Office or any firm contracted to process the data, will be held on a secure system that has been assured as part of the Cabinet Office's information assurance and risk management process.

92. All data provided for the purpose of **data matching exercises** will be backed up by Audit Scotland, or the Cabinet Office or any **data processor** undertaking data matching as its agent, at appropriate intervals, as reasonably necessary. Back-ups will be subject to the same security and access controls as the original data.

Use of third-party systems and suppliers

93. Where Audit Scotland or the Cabinet Office makes use of third-party systems or suppliers to support data matching exercises, those suppliers will act only on documented instructions and under contractual arrangements that ensure compliance with this Code and data protection legislation. Such suppliers must not use the data or the results of data matching for any purpose other than supporting the exercise, and must be subject to appropriate oversight, security controls and audit.

Use of application programming interfaces (APIs)

94. In some cases, data may be provided to, or matching results accessed from, the National Fraud Initiative systems through secure application programming interfaces (APIs). The use of APIs is a technical means of transferring data and does not alter the legal basis for data sharing, the roles and responsibilities of data controllers and processors, or the requirements of this Code. Data shared or accessed via APIs must be limited to what is necessary for the data matching exercise, protected by appropriate technical and organisational security measures, and used only for permitted purposes in accordance with this Code and data protection legislation.

Use of advanced analytics and emerging technologies

95. Data matching exercises may make use of a range of analytical techniques to identify potential matches, anomalies or inconsistencies, including more advanced or automated analytical tools. Regardless of the technology used, the purpose of data matching remains to assist in the prevention and detection of fraud or other permitted purposes, and no action should be taken solely as a result of automated processing. Data matching results are indicators only and must always be subject to

appropriate human review and judgement before any decision is made. Audit Scotland and participants must ensure that the use of such techniques is proportionate, transparent, and consistent with data protection legislation and the principles set out in this Code.

Access to the results by the bodies concerned

96. All results from **data matching exercises** will be made available to **participants** via the Cabinet Office's secure NFI website or authorised **APIs**. The results comprise the computer data file of reported matches and other relevant information arising from processing the data. The **senior responsible officer** should ensure that the results of a data matching exercise are disclosed only to named officers for each type of result. The secure NFI website is designed for that purpose.

97. All results from data matching exercises held by a participant other than on the secure NFI website should be secured in line with the NFI Security Policy that is provided on the secure NFI website. Any printed results should be kept in locked storage in a secure environment and should only be accessible to named individuals as referred to in the third bullet of paragraph 71.

98. Where the participant is sharing data under the **point of application** data sharing agreement the participant and service provider are responsible for the security of all information viewed or extracted from the system and are responsible for ensuring appropriate security controls are implemented. The Cabinet Office is only responsible for the security of the information up to the web-portal interface and is not responsible for the security of the participant and service provider end-point systems that view or extract the information on the portal.

99. The Cabinet Office and **data processor** shall on Audit Scotland's behalf ensure that procedures and system security controls are in place relating to information disclosed for data matching that reflect the provisions in this Code and **data protection legislation**. The Cabinet Office and data processor will:

- make accidental compromise of, damage to, or loss of the information unlikely during processing, storage, handling, use, transmission or transport
- deter deliberate compromise, or opportunist attack, and
- dispose of or destroy personal data in a manner to make reconstruction unlikely.

100. The **participant** shall ensure that the systems used to connect to the NFI web portal do not pose any security risk to the NFI system. Any data traffic that is identified or regarded as malicious by Audit Scotland, the Cabinet Office or their **data processor** may result in the connection to the participant being severed immediately.

Following up the results

101. The detailed steps taken by a participant to investigate the results of data matching are outside the scope of this Code. However, it is important to recognise that matches are not necessarily evidence of fraud or any other outcome related to the purpose for which the matching was undertaken. Participants should review the results to eliminate coincidental matches and will want to concentrate on the strongest cases that are potentially fraudulent or otherwise indicative of the outcome for which the matching was undertaken. They will also have to exercise caution in validating information in a match before taking action. In the process, they will need to identify and correct those cases where errors have occurred.

102. No decision should be made as a result of a data match until the circumstances have been considered by an investigator at the participant's organisation. Investigating officers will find it helpful to refer to the guidelines on how to interpret matches and cooperation between bodies prepared by the Cabinet Office, which are available to participants on its secure NFI website.

103. Participants should consider whether any corrections to personal data found to contain errors as a result of data matching are substantial enough to warrant notification to the persons concerned in line with the requirements of **data protection legislation** and any guidance issued by the Information Commissioner in this respect.

104. Participants should notify Audit Scotland of any amendments to personal data to correct substantial errors so that the NFI data can be amended to prevent further matches being generated due to the error.

Disclosure of data used in data matching

105. Data obtained for the purpose of a **data matching exercise** may not be disclosed unless there is legal authority for so doing. This applies to both data obtained by Audit Scotland for the purposes of data matching exercises and the results of the data matching.

106. There is legal authority for Audit Scotland to disclose the data or results when this will assist in the prevention and detection of fraud or another permitted purpose. This includes, for example, disclosure of the results to the **participant** to investigate any matches, and disclosure to the auditor, for example, to assess the participant's arrangements for the prevention and detection of fraud.

107. Audit Scotland may also provide data or data matching results, for example, to the NHS Counter Fraud Service in Scotland which has the connected purpose, among other things, of assisting health bodies to interpret and follow up the results of Audit Scotland's **data matching exercises**.

108. Audit Scotland may also disclose data to the Cabinet Office and other public sector audit agencies in Wales and Northern Ireland, to the bodies whose accounts they arrange to be audited, and to the auditors they appoint.

109. A body in receipt of data matching results from Audit Scotland may only disclose them further if it is to assist in the prevention and detection of fraud or another permitted purpose, to investigate and prosecute an offence, for the purpose of disclosure to an auditor or otherwise as required by statute.

110. The legal basis of these rules is Section 26D of the Public Finance and Accountability (Scotland) Act 2000. Any disclosure by Audit Scotland, a participant or any person in breach of Section 26D is a criminal offence.

Access by individuals to data included in data matching

111. Individuals whose data is included in a data matching exercise have rights under **data protection legislation** for confirmation that their data is being processed, access to their personal data and access to other supplementary information (which largely corresponds with the information that should be provided in a privacy notice). Request for personal data from the data subject should be dealt with in accordance with the organisation's general arrangements for responding to these requests. These requests should be dealt with without undue delay and within a month, unless the request is complex or numerous, where it is possible to extend the time by a further two months. Further guidance is available from the Information Commissioner in this respect.

112. Individuals' usual rights of access to data held about them may be limited as a consequence of exemptions from data protection legislation where disclosure would be likely to prejudice the prevention or detection of a crime or the apprehension or prosecution of an offender. This determination should be made on a case-by-case basis by the organisation in receipt of the request for information. This means that individuals may be refused full access to information about them that has been processed in data matching exercises.

113. Individuals have rights under **data protection legislation** if data held about them is inaccurate. They should be able to check the accuracy of their data by contacting the **participant** holding the data.

114. Individuals should not expect to be told about data or data matches concerning any other person unless that person has given consent, as this is likely to amount to a breach of data protection principles.

115. There are also rights to other information under the Freedom of Information (Scotland) Act 2002. Information requests under the Freedom of Information (Scotland) Act 2002 may be subject to the law enforcement exemption in Section 35, for example where its disclosure would be likely

to substantially prejudice the prevention and detection of a crime or the apprehension or prosecution of an offender, or the personal information exemption under Section 38. These determinations should be made on a case-by-case basis by the organisation in receipt of the request for information.

116. Individuals who want to know whether their data is to be included in a **data matching exercise** can check the data specifications for each exercise in Audit Scotland's instructions. The most up-to-date instructions can be found on Audit Scotland's website or by contacting Audit Scotland (see paragraph 24 for contact details).

117. Participants should have arrangements in place for dealing with complaints from individuals about their role in a data matching exercise. If a participant receives a complaint and Audit Scotland is best placed to deal with it, the complaint should be passed on promptly to Audit Scotland.

118. Complaints about Audit Scotland's role in conducting data matching exercises will be dealt with under Audit Scotland's complaints procedure (see paragraph 26 for details).

Role of auditors

119. Where a participant is an **audited body** to which the AGS or the Accounts Commission appoints an auditor, the auditor will be concerned, among other things, to assess the arrangements that the body has in place to:

- prevent and detect fraud generally
- follow up and investigate NFI matches and act upon instances of fraud.

120. Where a participant does not have an auditor appointed by the AGS or the Accounts Commission, it is a matter for the participant and its auditor to determine the role of the auditor in data matching and what disclosure to the auditor is appropriate.

Retention of data

121. Personal data should not be kept for longer than is necessary.

122. Access to the results of a **data matching exercise** on the secure NFI website will not be possible after a minimum reasonable period necessary for **participants** to follow up matches. Audit Scotland (or the Cabinet Office on its behalf) will notify the end date of this period to participants. A Data Deletion Schedule setting out the criteria for retaining and deleting data and matches will be published, and regularly updated, by the Cabinet Office on GOV.UK.

123. Participants and their auditors may decide to retain some data after this period. Data may, for example, be needed as working papers for the purposes of audit, or for the purpose of continuing investigation or prosecution. Participants should consider what to retain in their individual circumstances in the light of any particular obligations imposed on them. **Mandatory participants**, to which the AGS or Accounts Commission appoints an auditor, should discuss with their auditor what should be retained for the purposes of audit. All participants should ensure that data no longer required, including any data taken from the secure NFI website or shared via the NFI **API**, are destroyed promptly and rendered irrecoverable. Data retained will be subject to the requirements of **data protection legislation**.

124. All original data transmitted to Audit Scotland (or the Cabinet Office on its behalf), including data derived or produced from that original data and data held by any authorised data processors, will be retained for ongoing use across other NFI products. This data is refreshed every two years or upon receipt of new datasets from the subsequent national exercise, and it will be retained within the system until superseded by new data submissions to ensure effective ongoing fraud detection.

125. A single set of reference codes for previous matches, together with any comments made by participants' investigators, will be retained securely as a hashed algorithm by the Cabinet Office for as long as they are relevant. These codes are solely for the purpose of preventing unnecessary re-investigation of previous matches in any subsequent data matching exercise.

Reporting of data matching exercises

126. Audit Scotland will prepare and publish a report on its data matching exercises from time to time. This will bring its data matching activities and a summary of the results achieved to the attention of the public.

127. Audit Scotland's report will not include any information obtained for the purposes of data matching from which a person may be identified, unless the information is already in the public domain. Audit Scotland may report on the progress of prosecutions resulting from data matching as these will be in the public domain. Case studies will be used where the details are in the public interest.

Review of data matching exercises

128. Audit Scotland, in conjunction with the Cabinet Office, will review the results of each exercise in order to refine how it chooses the data for future exercises and the techniques it uses.

129. As part of its review of each exercise, Audit Scotland should consider any complaints or representations made by participants or by people whose data has been processed during the exercise.

3. Compliance with the Code and the role of the Information Commissioner

Compliance with the Code

130. Questions and concerns about non-compliance with the Code should be addressed to the organisation responsible in the first instance (that is to the **participant** or, if it concerns Audit Scotland's compliance, to Audit Scotland), before contacting the Information Commissioner. Participants may wish to raise any concerns they have with their own data protection officer in the first instance.

131. Where Audit Scotland or an auditor becomes aware that a participant has not complied with the requirements of the Code, they should notify the body concerned and seek to ensure that it puts in place adequate measures to meet the Code's requirements. For example, this might include where a participant has not issued adequate privacy notices.

Role of the Information Commissioner

132. The Information Commissioner regulates compliance with **data protection legislation**. The NFI's Code can be read alongside the Information Commissioner's data sharing code of practice. If a matter is referred to the Information Commissioner, they would consider compliance with this Code by participants or Audit Scotland in determining whether or not, in the view of the Information Commissioner, there has been any breach of data protection legislation and where there has been a breach, whether or not any enforcement action is required and the extent of such action. Guidance on the Information Commissioner's approach to data breaches and enforcement is available on the Information Commissioner's website.

133. Questions about data protection law and information sharing generally may be addressed to the Information Commissioner. In the first instance, public bodies in Scotland are advised to contact the Information Commissioner's regional office at:

The Information Commissioner's Office – Scotland
6th Floor
Quartermile One
15 Lauriston Place,
Edinburgh
EH3 9EP

The ICO's headquarters are at:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ICO helpline: 0303 123 1113

Email: icocasework@ico.org.uk

Website: www.ico.org.uk (use online enquiries form for questions regarding the legislation for which the Information Commissioner is responsible).

134. The Information Commissioner may be invited to review the Cabinet Office's (and, in effect, the NFI exercises undertaken by Audit Scotland and the other UK public sector audit agencies) data matching processes from time to time, to assess compliance with **data protection legislation**.

135. **Participants** are encouraged to invite the Information Commissioner's Office to review their procedures. The purpose of this review would be to assess participants' compliance with data protection principles when processing personal data for the purposes of **data matching exercises**. Further information can be found at: UK GDPR guidance and resources | ICO

Appendix

Definitions of terms used in the Code

For the purposes of this Code the following definitions apply:

Term	Definition
Application programming interface (API)	In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols and tools for building software and applications.
Audited body	A local government or other body in Scotland to which the AGS or the Accounts Commission appoints the auditor. This includes councils, police and fire and rescue authorities, health bodies, Scottish Government and other bodies in the central government sector. Lists of audited bodies and auditors are available on Audit Scotland's website.
Batch matching	Matching a large number of records from multiple data sets.
Data controllers	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data matching exercise	The comparison of sets of data to determine how far they match (including the identification of any patterns and trends). The purpose of data matching is to identify inconsistencies that may indicate fraud. A NFI data matching exercise may range from one application submission through to the full national exercise batch matching.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.
Data protection legislation	As defined in Section 3(9) of the Data Protection Act 2018 (DPA) and includes the DPA as well as the General Data Protection Regulation 2016/679 (GDPR) and relevant regulations.
Key contact	The officer nominated by a participant's senior responsible officer to act as point of contact with Audit Scotland and auditors for the purposes of data matching exercises.
Mandatory participant	An audited body or other person specified in Section 26C of the Public Finance and Accountability (Scotland) Act 2000 that is required by Audit Scotland to provide data for a data matching exercise.

Term	Definition
Participant	An organisation that provides data to Audit Scotland for the purposes of a data matching exercise, which may be on either a mandatory or voluntary basis.
Patient data	Data relating to an individual that are held for medical purposes and from which the individual can be identified. This includes both clinical data (eg, the medical records), and demographic data (eg, the name and address) of patients and care recipients.
Personal data	Data relating to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Point of application matching	Cross-checking information provided by applicants for benefits, goods or services against other datasets at the time the application is made, for example, the NFI AppCheck facility.
Senior responsible officer	The Director of Finance or other senior named officer of the participant responsible for ensuring compliance with this Code.
Voluntary participant	An organisation from which Audit Scotland considers it appropriate to accept data on a voluntary basis for the purposes of data matching.

Draft Code of data matching practice 2026

Issued under Section 26F of the Public Finance and Accountability (Scotland) Act 2000

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500
www.audit.scot

AS.5.0