

National Fraud Initiative (NFI) Privacy Notice

We are required by law to protect the public funds we administer. We may share information provided with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud. The Cabinet Office is responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to determine the extent of the match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

We participate in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud – see guidance <https://www.gov.uk/guidance/taking-part-in-national-fraud-initiative>. We want you to know that we take privacy very seriously. Please be assured that we will always manage your data securely and responsibly. See private notice guidance which sets out how we will use your personal data as part of the Cabinet Office's National Fraud Initiative (NFI) data matching exercise to aid in the prevention and detection of fraud [Privacy notice - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/privacy-notice-national-fraud-initiative).

The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under data protection legislation or the General Data Protection Regulation (GDPR). For further information on how we will use your personal data, and your rights, see [National Fraud Initiative privacy notice - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/national-fraud-initiative-privacy-notice). For further information on the reasons why it matches particular information, see [Code of Data Matching Practice for the National Fraud Initiative - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/code-of-data-matching-practice-for-the-national-fraud-initiative)

For further information on data matching at Sandwell and West Birmingham Hospitals NHS Trust contact Manjit Sandhu, Local Counter Fraud Specialist, by emailing manjit.sandhu@rsmuk.com. Further information on how the NFI has assisted the NHS and other public sector organisations can also be found at [National Fraud Initiative case studies - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/national-fraud-initiative-case-studies)

Useful resources:

Your organisation's privacy notice

[National Fraud Initiative privacy notice - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/national-fraud-initiative-privacy-notice)

[Right to be informed | ICO](https://ico.org.uk/your-data-matters/right-to-be-informed/)

[A guide to the data protection exemptions | ICO](https://ico.org.uk/your-data-matters/a-guide-to-the-data-protection-exemptions/)

[Getting copies of your information \(SAR\) | ICO](https://ico.org.uk/your-data-matters/getting-copies-of-your-information-sar/)

[NFI Security Policy.pdf](#)