

Staff Privacy Notice

Everyone working for the ICB has a legal duty to keep personal information confidential, which includes that of staff members.

This Privacy Notice describes how the ICB uses and processes the information it holds about its staff, including how the information may be shared with other organisations, and how the confidentiality of staff information is maintained.

The ICB is registered with the Information Commissioner's Office (ICO) as a data controller and collects data for a variety of purposes; further information can be obtained here [Register of fee payers | ICO](#)

For the purposes of this Privacy Notice "staff" includes all employees, including but not limited to, permanent staff, agency, contract and temporary staff, volunteers and students.

The Privacy Notice should be read in conjunction with your contract of employment and local policies and procedures.

Why is information recorded about me?

We only collect and use your information for the lawful purposes of administering the business of the ICB. These purposes include:

- To improve the management of workforce data;
- To inform the development of recruitment and retention policies;
- To allow better financial modelling and planning;
- To enable monitoring of ethnicity, sexual orientation, disability and other protected characteristics;
- To keep images to identify you either as part of the various security access systems, including CCTV and for identity cards;
- To keep images that appear in the ICB or other publications or websites to market and promote the ICB;
- To allow the ICB policies to be implemented and acted upon when appropriate;
- To assist in the prevention and detection of fraud;
- To keep records of ICB meetings to allow transparency for decision making.

There are many reasons linked to staff administration of your employment such as paying you and processing any changes that happen as a result of your career development.

What information is collected about me?

In order to carry out our activities and obligations as an employer we handle information about you in relation to:

OFFICIAL

- Personal details such as name, address, telephone number(s), date of birth
- Personal demographics (including gender, race, ethnicity, sexual orientation, religion)
- Medical information (including physical and/or mental health)
- Emergency contact(s), eg next of kin details
- Education and training
- Employment details (including job role, place of work, references and proof of eligibility to work in the UK)
- Membership of professional bodies and/or trade union(s)
- Bank details, eg in order to pay your salary
- Pension details
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Employment tribunal applications, complaints, accidents and incident details
- Visual images, e.g. photographs or CCTV monitoring
- Audio recordings of 'in public' meetings
- Personal Development Plans and appraisal documentation
- Sickness absence and annual leave details
- Declarations of Interest

You should be aware that once you have approved your image to appear in a publication or on an internet platform (usually done verbally) we may not be able to completely retrieve this image if you change your mind about its use. Your image may appear again at a later date unless you specifically indicate otherwise.

We may use your information in order to gather evidence for disciplinary and other staff processes. The use of this information will always be proportionate in relation to the evidence being sought.

How is Information kept about me?

Your information is stored in both paper (personal files held by your line manager or HR team) and electronically on ESR. Other temporary files may be created as a result of investigations, disciplinarys or complaints but these will be incorporated into the personal file upon completion.

How long do you hold information for?

All records held by the ICB will be kept for the duration specified by national guidance from the Department of Health, *The Records Management Code of Practice 2021*. Confidential information is securely destroyed in accordance with this code of practice.

Who do you share my information with?

We will not routinely disclose any information about you to anyone outside the ICB without your consent. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation. We may obtain and share personal information with a wide variety of other bodies, which may include, but is not limited to:

- Her Majesty's Revenue and Customs (HMRC)
- Department for Work and Pensions (DWP)
- Disclosure and Barring Service (DBS)
- Home Office
- Child Support Agency
- Regulatory bodies, e.g. Nursing and Midwifery Council, General Medical Council

- Law enforcement agencies including the Police and the Serious Organised Crime Agency
- NHS Protect/NHS Counter Fraud
- Auditors
- Northumbria Healthcare NHS Foundation Trust
- North of England Commissioning Support
- Electronic Staff Records (ESR) (IBM)
- NHS Business Services Authority (BSA)

If you post or send offensive, inappropriate or objectionable content anywhere on social media, or otherwise engage in any disruptive behaviour we may use whatever information is available to us, about you, to stop such behaviour.

How can I access my information?

You can request access to the information that the ICB holds about you and you should do this by approaching your line manager in the first instance. A procedure is available called Subject Access Request and Data Subject Rights SOP. Your request, once agreed with you, will be completed within 30 calendar days. However, if your records are extensive we may take longer to process your request but will inform you from the outset.

To submit a formal request, please contact:

Information Governance Team
John Snow House
Durham University Science Park
Durham
DH1 3YG

Or email: necsu.icbfoi@nhs.net

Information that you are entitled to:

As well as receiving a copy of the information that the ICB holds and processes you are also entitled to the following:

- To be told whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Given a copy of the personal data together with its source (where this is available).

How do you make sure it is safe and secure?

We will use your information in a way that follows data protection laws and the ICB policies and procedures.

Everyone working for the NHS is subject to the Common Law Duty of Confidence. Information provided in confidence will only be used for the purposes advised and consented to, unless it is required or permitted by the law.

All ICB staff are required to undertake mandatory Information Governance training, which covers how personal information should be kept secure.

We do not transfer your personal information to a country outside of the European Union (EU) and this is checked on a yearly basis. If it is found that we intend to share information outside of the EU, appropriate and suitable safeguards will be put in place, which you will be told about.

How do you protect my privacy/confidentiality?

We protect your information by following data protection laws:

- General Data Protection Regulation (GDPR) (applies from May 2018)
- Data Protection Act (DPA) 2018

The GDPR 2016 and DPA 2018 are the laws that primarily determine how we can use your personal data. However, there are other laws that are followed if we need to process your information:

- The Human Rights Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1998
- Audit Commission Act 1998
- Regulation of Investigatory Powers Act 2000

What are my rights?

Where information from which you can be identified is held, you have the right to ask to:

- View this or request copies of the records by making a subject access request.
- request information is corrected
- have the information updated where it is no longer accurate
- ask us to stop processing information about you where we are not required to do so by law – although we will first need to explain how this may affect you.

GDPR introduced further rights in addition to the above such as the right to erasure of information, restriction of processing, automated decision-making and profiling.

Further Information

Data Protection Officer

The Data Protection Officer (DPO) is responsible for ensuring that the ICB complies with the GDPR. The DPO is the person to contact if you would like to know more about how we use your information, require information in any accessible format or language or if (for any reason) you do not wish to have your information used in any of the ways described. The DPO contact details are:

Liane Cotterill
Data Protection Officer
John Snow House
Durham University Science Park
Durham
DH1 3YG
Or email to liane.cotterill@nhs.net

Caldicott Guardian

The Caldicott Guardian is the person who makes the final decision on how, what, when and why personal information will be processed in/by the ICB. The ICB's Caldicott Guardian is Dr Neil O'Brien, Executive Medical Director.

For independent advice about data protection, privacy and information-sharing issues you can contact the Information Commissioner:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow,
December 2022

Cheshire
SK9 5AF
Phone: 08456 30 60 60 or 01625 54 57 45
Website: www.ico.org.uk