# Sheffield Children's NHS Foundation Trust privacy notice for the NHS Digital Staff Passport

This privacy notice tells you what to expect us to do with your personal information when you contact us or use our services.

You can find more detailed information about how we use your information for the following specific purposes here:

- The Digital Staff Passport (DSP)

## Our contact details

Name: Sheffield Children's NHS Foundation Trust

General enquiries email address:

Where we are your current employer, we are the controller for your information. A controller decides on why and how information is used and shared.

Where we are your 'new' or future employer, we will become the controller of any records created using your Digital Staff Passport.

## Data Protection Officer contact details

Our Data Protection Officer is Mark Talbot and is responsible for monitoring our compliance with data protection requirements. You can contact them with queries or concerns relating to the use of your personal data at scn-tr.dataprotection@nhs.net.

## How do we get information and why do we have it?

The personal information we collect is provided directly from you for one of the following reasons:

- you have applied for a job with us or work for us, and
- you have chosen to use the NHS Digital Staff Passport.

We also receive personal information about you indirectly from others, in the following scenarios:

- from other health and care organisations you are employed with, through the Electronic Staff Record (ESR), to speed up pre-employment checks when you move between NHS organisations.

## What information do we collect?

### Personal information

We currently need the following personal information to provide your Digital Staff Passport:

- basic personal details about you – your name, address, date of birth, email address and

an ID photo of you
- basic details relating to your work status – Disclosure and Barring Service (DBS) information, right to work information (residency/visa), your professional registration details (such as the General Medical Council, Nursing and Midwifery Council, General Dental Council or Health and Care Professions Council), your ESR assignment number
- clinical training and qualification details, any other specific clinical skills, and any restrictions on your practice
- basic details relating to your current employment – employing organisation, job role, staff group, department, start date, pay band, work email address, area of work, job title
- details of any supporting evidence or document e.g. passport number, driving licence number

You can also choose to provide the following additional optional information:
- maiden name or previous name
- preferred pronouns
- phone number
- country of birth
- next of kin or emergency contact details
- marital status

**More sensitive information**
We need the following more sensitive data to provide your Digital Staff Passport:

- limited healthcare information relating to your employment – specifically, occupational health clearance status

We process the following more sensitive data where you have chosen to provide it:

- data revealing racial or ethnic origin
- data concerning a person's sexual orientation
- data revealing religious or philosophical beliefs
- immunisation, vaccine and testing data in relation to tuberculosis (TB) and varicella (to be extended in the future)

## Who do we share information with?

Information will be shared with NHS England, who will host the data, and who will also remove any identifiers (such as your name) to then use the data to analyse the service and for reporting purposes. NHS England data engineers may also be granted access to the data in limited circumstances, such as in the case of an investigation.

NHS England will also work with a carefully selected third party (Sitekit Ltd) to provide technical support for the Digital Staff Passport.

Sitekit will not routinely have access to your personal data. There may however be occasions where personal data is shared with Sitekit if technical support is needed.

Your information will also be shared with organisations, such as Yoti and Microsoft (through the Authenticator app), who will verify your identity to ensure that it is in fact you who is requesting access to your Digital Staff Passport.

## Is information transferred outside the UK?

Some of your login data (specifically forename, surname and email address) is securely stored on data servers in European countries covered by the EU General Data Protection Regulations.

## What is our lawful basis for using information?

**Personal information**

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for using personal information are:

(c) We have a legal obligation - the Employment Rights Act 1996 sets out requirements for employers in relation to their employees. This includes keeping records of staff when working for them.

(e) We need it to perform a public task - See this list for the most likely laws that apply when using and sharing information in health and care. This legal basis applies to the information that is not subject to a legal obligation but is provided by you to support us as your employing organisation in the performance of our public task.

**More sensitive data**

Under UK GDPR, the lawful basis we rely on for using information that is more sensitive (special category):

(b) We need it for employment, social security and social protection reasons (if authorised by law). See this list for the most likely laws that apply when using and sharing information in health and care.

### Common law duty of confidentiality

In our use of health and care information, we satisfy the common law duty of confidentiality because:

- you have provided us with your consent upon agreeing to the terms and conditions of the use of the Digital Staff Passport.

## How do we store your personal information?

Your data will be stored by NHS England in the Microsoft Azure cloud. When you download your passport to your mobile device, your passport details will be held within the Microsoft Authenticator digital wallet app. Both storage locations have robust security measures in place to ensure your data is safe and secure.

Your data will be held for as long as your Digital Staff Passport is active. If you temporarily disable your passport, your data will be retained so that the process for reactivating your Digital Staff Passport is convenient for you. However, if you permanently delete your Digital Staff Passport account, your data will be deleted.

## What are your data protection rights?

Under data protection law, you have rights including:

**Your right of access** - You have the right to ask us for copies of your personal information (known as a subject access request). You can view your information on the Digital Staff Passport system.

**Your right to rectification** - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. You can edit your own information on through the Digital Staff Passport system.

**Your right to erasure** - You have the right to ask us to erase your personal information in certain circumstances. You can do this by deleting your Digital Staff Passport account.

**Your right to restriction of processing** - You have the right to ask us to restrict the processing of your personal information in certain circumstances. You can do this by deleting your Digital Staff Passport account.

**Your right to object to processing** - You have the right to object to the processing of your personal information in certain circumstances. You can do this by deleting your Digital Staff Passport account.

**Your right to data portability** – this right to ask that we transfer the personal information you gave us to another organisation, or to you, does not apply in this circumstance.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at scn-tr.dataprotection@nhs.net if you wish to make a request.

### National data opt-out

- we are not applying the national data opt-out because we are not using confidential patient information for planning or research purposes

## How do I complain?

If you have any concerns about our use of your personal information, you can make a complaint to us at scn-tr.dataprotection@nhs.net.

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO's address is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow

Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: www.ico.org.uk

**Date of last review**

Version 1.0, 05/07/2024