



Staff Privacy Notice

Printed copies should not be considered the definitive version.



Data Protection Notice

During the course of NHS Greater Glasgow and Clyde activities we will collect, store and process personal information about our prospective, current and former staff. For the purposes of this privacy notice, 'staff' includes applicants, employees, workers (including independent practitioners, bank, agency, casual and contracted staff), volunteers, trainees and those carrying out work experience.

We recognise the need to treat staffs' personal data in a fair and lawful manner. No personal information held by us will be processed unless the requirements for fair and lawful processing can be met. This privacy notice provides a summary of how we will ensure that we do that, by describing the:

- Categories of personal data we may handle
- Person(s) it may be shared with and
- Purpose(s) for which it is being processed.

This notice also explains what rights you have to control how we use your information. Please read it carefully to understand what we do.

This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with a link to the updated copy of this notice as soon as reasonably practical.

It is important that you read and can easily access this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

What laws are relevant to the handling of personal information?

The law determines how organisations can use personal information. The key legislation governing the use of information is listed below:

- Access to Health Records 1990
- Computer Misuse Act 1998
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- General Data Protection Regulation (GDPR (EU) 2016/679)
- Human Rights Act 1998 and
- Regulation of Investigatory Powers Act 2000



NHS Greater Glasgow and Clyde (NHSGGC) is the 'Data Controller' (the holder, user and processor) of staff information.

What types of personal information do we handle?

In order to carry out our activities and obligations, as an employer we handle data in relation to personal data disclosed and any other information necessary for our business purposes, which is provided in the course of an employee's application for and during employment with us. This includes:

- Absence information, e.g. annual leave, sickness absence, study leave, maternity leave, paternity leave
- Bank account details, payroll records and tax status information
- CCTV data
- Compensation history
- Copy of driving licence
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships)
- Gender
- Information about your use of our information and communications systems
- Leaving data and your reason for leaving
- Location of employment or workplace
- Marital status and dependants
- Name, home address, telephone, personal email address, date of birth, employee identification number and marital status, and any other information necessary for our business purposes, which is voluntarily disclosed in the course of an employee's application for and employment with us
- National insurance number
- Next of kin and emergency contact information
- Occupational health clearance information
- Performance information
- Photographs
- Qualification and training information;
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied



- Salary, annual leave, pension and benefits information
- Start date and, if different, the date of your continuous employment
- Statutory and voluntary registration data and
- Swipe access cards and other secure access technology (including finger-print recognition).

We may also collect, store and use the following ‘special categories’ of more sensitive personal information which may include information about:

- Health, including any medical condition, health and sickness records, including:
 - Details of any absences (other than holidays) from work including time on statutory parental leave and sick leave
 - Where you leave employment and the reason for leaving is related to your health, information about that condition needed for pension purposes.
 - Genetic information and biometric data (including for secure access technology)
 - Information about criminal convictions and offences
- Race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership

When you are no longer our employee, we may continue to share your information as described in this notice, so long as this is fair and lawful.

What is the purpose of processing data?

Your personal data is collected by NHSGGC and shared with NHS Scotland for the purposes of employee management. It will be captured and stored on an electronic system and will be used and shared by human resource (HR) professionals in NHSGGC and Board(s) where you are working in any capacity with relevant parties.

We collect personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

Occupational health clearance information – referred to as the Occupational Health Passport – will be shared by NHSGGC with occupational health professionals in the Board, and Boards where you have been offered employment.

We will only use your personal information when the law allows us to. Most commonly we will use your personal information in the following circumstances to:



- Administer termination of employment and provide and maintain references;
- Comply with applicable laws (e.g. health and safety), including judicial or administrative orders regarding individual employees (e.g., child support payments);
- Develop workforce and succession plans;
- Evaluate applications for employment;
- Maintain emergency contact and beneficiary details, which involves us holding information on those nominated by you;
- Maintain sickness records, and occupational health programme;
- Manage all aspects of your employment with us, including but not limited to, payroll, benefits, corporate travel and other reimbursable expenses, development and training, absence monitoring, performance appraisal, disciplinary and grievance processes, pensions administration, and other general administrative and human resource related processes;
- Share and match personal information for the national fraud initiative and
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- where we need to protect your interests (or someone else's interests)
- where it is needed in the public interest or for official purposes

We use information about you in order to perform our contract with you [❖] and to enable us to comply with our legal obligations [■]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties [○], provided your interests and fundamental rights do not override those interests.

The situations in which we will process your personal information are listed below. We have indicated by asterisks the purpose or purposes for which we are processing or will process your personal information, as well as indicating which categories of data are involved.

- ❖ Administering the contract we have entered into with you;
- ❖ Ascertaining your fitness to work;
- ❖ Assessing qualifications for a particular job or task, including decisions about promotions;
- ❖ Conducting performance reviews, managing performance and determining performance requirements;
- ❖ Determining the terms on which you work for us;
- ❖ Education, training and development requirements;
- ❖ Gathering evidence for possible grievance or disciplinary hearings;



- ❖ Maintain sickness records and Occupational Health Programme;
 - ❖ Making a decision about your recruitment or appointment;
 - ❖ Making arrangements for the termination of our working relationship;
 - ❖ Making decisions about your continued employment or engagement;
 - ❖ Manage all aspects of your employment with us, including but not limited to, payroll, benefits, corporate travel and other reimbursable expenses, development and training, absence monitoring, performance appraisal, disciplinary and grievance processes, pensions administration, and other general administrative and human resource related processes;
 - ❖ Managing sickness absence;
 - ❖ Monitor your use of our information and communication systems to ensure compliance with our IT policies, including physical access rights.
 - ❖ Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs);
-
- Checking you are legally entitled to work in the UK;
 - Comply with any Court Order which may be imposed.
 - Comply with current legislation e.g. ensure appropriate use of records, which is monitored via Fairwarning;
 - Complying with health and safety obligations;
 - Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
 - Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties;
 - Equal opportunities monitoring;
 - Maintain emergency contact details to comply with applicable laws (e.g. health and safety), including judicial or administrative orders regarding individual employees (e.g., child support payments);
-
- Business management and planning, including accounting and auditing;
 - Conduct data analytics studies to review and better understand employee retention and attrition rates;
 - Develop workforce and succession plans.
 - Ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
 - Evaluate applications for employment;



- Liaising with the trustees or managers of a pension arrangement operated by the SPPA, your pension provider and any other provider of employee benefits;
- Provide and maintain references;
- Share and match personal information for fraud prevention.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

Any disclosures of personal data are always made on case-by-case basis, using the personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a legal requirement or where you have consented to the disclosure of your personal data to your representative.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require appropriate levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to an occupational pension scheme.



Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Our obligations as an employer

We may use your particularly sensitive personal information in the following ways:

- Information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance;
- Information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting;
- Information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws;
- If you apply for an ill-health pension under a pension arrangement operated by the SPPA, we will provide information about your physical or mental health to SPPA in order for them to reach a decision about your entitlement;
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?

We do not need your consent if we use special categories of your personal information to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

In order to comply with our obligations as an employer we will need to share your information as follows:

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with Board policies.



Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences to assess your suitability for employment or to assess your suitability for continued employment.

We are allowed to use your personal information in this way to carry out our obligations as a public sector employer to ensure we comply with our legal obligations. We have in place an appropriate guidance to outline how we will process such data - <https://www.nhsggc.org.uk/working-with-us/hr-connect/recruitment-service/the-recruitment-process/recruitment-process-guidance-for-hiring-managers/recruiting-with-convictions/>.

Background on sharing and our responsibilities

Privacy laws do not generally require us to obtain your consent for the collection, use or disclosure of personal information for the purpose of establishing, managing or terminating your contract of employment. In addition, we may collect, use or disclose your personal information without your knowledge or consent where we are permitted or required by law or regulatory requirements to do so.

The GDPR and the Data Protection Act 2018 require personal data to be processed fairly and lawfully. In practice, this means that NHSGGC must ensure personal data is:

- Collected for specified explicit and legitimate purposes;
- Adequate relevant and limited to what is necessary;
- Accurate and where necessary kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed; and
- Processed in a manner that ensure appropriate security of the personal data.

NHSGGC's legal basis for collecting and using staff personal data and/or special category such as health information, is because it is necessary to do so when staff have an employment contract with the Board or potentially entering into an employment contract.

As such we believe our lawful basis is largely Article 6(1)(b) processing necessary for the performance of a contract; and for sensitive information Article 9(2)(b) processing necessary or the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment. This may also be:



- for occupational health and safety reasons or the assessment of your working capacity;
- for the establishment/exercise/defence of legal claims;
- to prevent fraud;
- to protect your vital interests or those of another person where you/they are unable to give consent;
- where the data has been made public by you.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

In order to comply with our obligations as an employer we may need to share appropriate, relevant and proportionate personal information in compliance with the law, with the following:

- Audit Scotland
- Councils
- Disclosure Scotland
- HMRC
- Other NHS Boards
- Regulatory Bodies
- Scottish Government
- Trade Unions

We may also need to share your personal information to otherwise comply with the law.

We will also share personal data regarding your participation in any pension arrangement, such as the SPPA pension scheme, with the trustees or scheme managers of that pension arrangement in connection with the administration of the arrangement.

Information about the rights of individuals under the Data Protection Legislation can be found within the NHSGGC Confidentiality and Data Protection Policy.

Security of your Information

We take our duty to protect your personal information and confidentiality very seriously and we are committed to taking all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper.

At director level, we have appointed a Senior Information Risk Owner (SIRO) who is accountable for the management of all information assets and any associated risks and incidents, and a Caldicott Guardian who is responsible for the management of patient information and patient confidentiality. We also have a Data Protection Officer who is responsible for the Boards data protection compliance and who liaises with the SIRO and Caldicott Guardian.



All staff are required to undertake regular information governance training and to be familiar with information governance policies and procedures.

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

How do we collect your information?

Your information will be collected on a national workforce information system. The national system manager is authorised for full access nationally, providing access and accounts for NHS Boards system administrators. NHSGGC has a number of staff in this role – all within HR.

We also collect information in a number of other ways, for example correspondence, forms, interview records, references and surveys.

Retaining information

We only keep your information for as long as it is necessary to fulfil the purposes for which the personal information was collected. This includes for the purpose of meeting any legal, accounting or other reporting requirements or obligations. The Scottish Government Records Management: NHS Code of Practice (Scotland) sets out the minimum retention timescales.

We may, instead of destroying or erasing your personal information, make it anonymous so that it cannot be associated with or tracked back to you.

Your rights

This section contains a description of your data protection rights within NHSGGC as an employee.

The right to be informed

NHSGGC must explain how we use your personal information. We use a number of ways to communicate how personal information is used, including:

- This Data Protection Notice
- Contract of Employment
- Staff managing you

How can you get access your personal data?

You have the right to access the information which NHSGGC holds about you, and why, subject to any exemptions. Requests can be made in a number of ways, including in writing or verbally. You will need to provide:



- Adequate information [for example full name, address, date of birth, staff number, etc.] so that your identity can be verified and your personal data located.
- An indication of what information you are requesting to enable us to locate this in an efficient manner.
- We may ask you to complete an application form to collect the data we need, although you are not obliged to do so.

You should direct your request to the Data Protection Officer – details can be found on page 16.

We aim to comply with requests for access to personal data as quickly as possible. We will ensure that we deal with requests within 30 days of receipt unless there is a reason for delay that is justifiable.

What if the data you hold about me is incorrect?

It is important that the information which we hold about you is up to date. Staff can amend some elements of personal information as required via the national workforce information system. If any other changes not accessible via this route are required then it is important that you let us know by contacting your manager or by contacting the HR Support and Advice Unit.

If the personal information we hold about you is inaccurate or incomplete you have the right to have this corrected.

If it is agreed that your personal information is inaccurate or incomplete we will aim to amend your records accordingly, normally within one month, or within two months where the request is complex. However, we will contact you as quickly as possible to explain this further if the need to extend our timescales applies to your request. Unless there is a risk to patient or staff safety, we can restrict access to your records to ensure that the inaccurate or incomplete information is not used until amended.

If for any reason we have shared your information with anyone else, we will notify them of the changes required so that we can ensure their records are accurate.

If on consideration of your request NHSGGC does not consider the personal information to be inaccurate then we will add a comment to your record stating your concerns about the information. If this is the case we will contact you within one month to explain our reasons for this.

If you are unhappy about how NHSGGC has responded to your request for rectification we will provide you with information on how you can complain to the Information Commissioner's Office.

The right to object

When NHSGGC is processing your personal information for the purpose of the contract of employment or performance of a task carried out in the public interest or in the exercise of official authority you have the right to object to the processing and also seek that further processing of your



personal information is restricted. Provided NHSGGC can demonstrate compelling legitimate grounds for processing your personal information or for evidence to support legal claims, your right will not be upheld.

The right to erasure

The right to erasure is also known as “the right to be forgotten” and in general refers to an individual’s right to request the deletion or removal of personal information where there is no compelling reason for NHSGGC to continue using it.

As with other rights, there are particular conditions around this right and it does not provide individuals with an absolute right to be forgotten.

Individuals have the right to have their personal information deleted or removed in the following circumstances:

- If there is a legal obligation to erase your personal information, for example by court order;
- If we have used your personal information unlawfully;
- When it is no longer necessary for the purpose for which it was collected;
- When NHSGGC no longer have a legal basis for using your personal information, for example if you gave us consent to use your personal information in a specific way, and you withdraw your consent, we would need to stop using your information and erase it unless we had an overriding reason to continue to use it;
- When you object to NHSGGC using your personal information and there is no overriding legitimate interest for us to continue using it.

NHSGGC can refuse to deal with your request for erasure when we use your personal information for the following reasons:

- Archiving purposes in the public interest;
- Public health purposes in the public interest;
- The exercise or defence of legal claims;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority.

When using personal information our legal basis is usually that its use is necessary for the performance of your contract of employment or a task carried out in the public interest or in the exercise of official authority vested in us under the NHS Scotland Act. This means that in most circumstances we can refuse requests for erasure. However we will advise you of this as soon as possible following receipt of your request.

The right to restrict processing

You have the right to control how we use your personal information in some circumstances. This is known as the right to restriction. When processing is restricted, NHSGGC are permitted to store



your personal information, but not further use it until an agreement is reached with you about further processing. We can retain enough information about you to ensure that your request for restriction is respected in the future.

Examples of ways you can restrict our processing would be:

- If our use of your personal information is found to be unlawful and you ask for restriction instead of full erasure we will restrict our processing;
- If we no longer need your personal information but you need it to establish, exercise or defend a legal claim, we will restrict our processing;
- If you challenge the accuracy of your personal information, we will stop using it until we check its accuracy;
- If you object to processing which is necessary for the performance of our tasks in the public interest or for the purpose of legitimate interests, we will restrict our processing while we consider whether our legitimate grounds override your individual interests, rights and freedoms

If we have shared your personal information with any individuals or organisations, if we restrict our processing, we will tell those individuals or organisations about our restriction if it is possible and not an unreasonable amount of effort. Whenever we decide to lift a restriction on processing we will tell you.

The right to data portability

The right to data portability allows individuals to obtain and re-use their personal information for their own purposes across different services. It allows them to move, copy or transfer personal information easily from one IT environment to another in a safe and secure way. For example, it enables consumers to take advantage of applications and services which can use their information to find them a better deal.

The right to data portability only applies when the individual has submitted their personal information directly, through electronic means to NHSGGC. This means that in most circumstances the right to data portability does not apply within NHSGGC.

Rights related to automated decision making and profiling

You have the right to object to any instances where a decision is made about you solely by automated means without any human involvement, including profiling.

NHSGGC does not undertake any decision-making about you using wholly automated means.

Your duty to inform us of changes



It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Freedom of Information

The Freedom of information (Scotland) Act 2002 provides any person with the right to obtain information held by NHSGGC, subject to a number of exemptions - personal data is normally exempt. If you would like to request information from us, please send your request to the Freedom of Information Manager at foi@ggc.scot.nhs.uk.

Any request to access personal data we hold about you will be handled under the Data Protection Act 2018 and GDPR.

Complaints about how we process your personal information

In the first instance, you should contact the Data Protection Officer – contact details can be found on page 16. Information about the rights of individuals under the Data Protection Act can be found online [click here](#)

Data Protection Notification

NHSGGC is a ‘data controller’ under the Data Protection Act. We have notified the Information Commissioner that we process personal data and our registration number is: Z8522787.

The details are publicly available from the:-

Information Commissioner’s Office
Wycliffe House
Water Lane,
Wilmslow SK9 5AF

www.ico.gov.uk

How to contact us

Please contact us if you have any questions about our privacy notice or information we hold about you:



Email: Data.Protection@ggc.scot.nhs.uk or

Isobel Brown
Data Protection Officer

NHS Greater Glasgow and Clyde
1 Smithhills Street
Level 2
Paisley
PA1 1EB

Or

Tel: 0141 278 4774