Eve Hill Medical Practice

Privacy Notice – Employee

Subject:	Privacy Notice - Employee
Date of Review:	16/03/2026
Date of Next Review:	16/03/2027
Person Responsible for Policy Implementation and Review:	Kelly Houseman – Practice Manager
Policy Location:	Teamnet/Library
Version	4

Table of contents

1 Introduction

1.1 Policy statement

This policy outlines how this organisation will provide information to staff regarding how their personal data is processed. Every staff member should be aware of the Employee Privacy Notice and understand how that information may be used and with whom the organisation will share that information.

This policy is to be read in conjunction with the organisation's UK General Data Protection Regulation (UK GDPR) Policy.

1.2 Status

In accordance with the Equality Act 2010, we have considered how provisions within this policy might impact on different groups and individuals. This document and any procedures contained within it are non-contractual, which means they may be modified or withdrawn at any time. They apply to all employees and contractors working for the organisation.

2 Compliance with regulations

2.1 Data Protection Act 2018 and UK GDPR

The General Data Protection Regulation (GDPR) became law on 24 May 2016. This was a single EU-wide regulation on the protection of confidential and sensitive information. It entered into force in the UK on the 25 May 2018, repealing the Data Protection Act (1998).

Following Brexit, the GDPR became incorporated into the Data Protection Act 2018 (DPA18) at Part 2, Chapter 2 titled The UK GDPR.

This organisation will ensure that any personal data is processed in accordance with Article 5 of the UK GDPR and information about how this is done will be provided to applicants in a format that is compliant with Article 12 of the UK GDPR.

2.2 Communicating privacy information

This organisation must provide information to applicants about how their data is processed in the form of an Employee Privacy Notice.

The privacy notice template is available at Annex A.

2.3 Use of artificial intelligence

Artificial Intelligence (AI) use is the biggest and fastest moving change to computing in recent years and is becoming commonplace across all industries including primary care. With this being new technology, there is a requirement for additional governance measures to ensure its use is safe and does not expose personal data about staff to any unnecessary risks.

An example where AI could be used to support day-to-day business activity is the generation of business meeting notes and any action points

For further information, including how this organisation will comply with the Data Protection Act 2018 and UK GDPR, refer to the organisation's Privacy Notice – Artificial Intelligence.

3 Further information

3.1 Privacy notice checklist

The Information Commissioner's Office has provided a privacy notice checklist that can be used to support the writing of this privacy notice.

Annex A – Employee privacy notice

Introduction

The organisation gathers and processes personal data relating to its employees to enable us to run the business and manage our relationship with you. We are committed to being open and transparent about how we gather and use that data and to meeting our data protection obligations.

This privacy notice applies to personal information processed by or on behalf of Eve Hill Medical Practice.

This notice explains:

- Who we are, how we use your information and our data protection officer (DPO)
- What kind of personal information about you we process
- What the legal grounds are for our processing of your personal information (including when we share it with others)
- What you should do if your personal information changes
- For how long your personal information is retained by us
- What your rights are under data protection laws

The General Data Protection Regulation (GDPR) became law on 24 May 2016. This was a single EU-wide regulation on the protection of confidential and sensitive information. It entered into force in the UK on the 25 May 2018, repealing the Data Protection Act (1998). Following Brexit, the GDPR became incorporated into the Data Protection Act 2018 (DPA18) at Part 2, Chapter 2 titled The UK GDPR.

For the purpose of applicable data protection legislation (including but not limited to the Data Protection Act 2018 (DPA2018) and Part 2 the UK GDPR)

This notice describes how we collect, use and process your personal data and how, in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

How we use your information and the law

This organisation will be what is known as the ‘controller’ of the personal data you provide to us. Upon applying for work with the organisation you will be asked to supply the following personal information:

- Name

- Address
- Telephone numbers
- Email address
- Date of birth
- Gender
- Marital status and family details
- National insurance number
- Bank details
- Emergency contact information
- Health information
- Vaccination and immunisation status/information
- Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments
- Information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement
- Your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us
- Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings)

- Information relating to your performance and behaviour at work
- Training records
- Electronic information in relation to your use of IT systems/swipe cards/telephone systems
- Your images (whether captured on CCTV, by photograph or video)

The information that we ask you to provide to the organisation is required for the following reasons:

- For us to pay your salary
- For us to contact you out of hours if required
- To provide you with organisation information via email and post if required
- To have the ability to contact your emergency contacts if necessary
- To ensure we are able to inform the emergency services if your health is compromised
- To ensure that we can provide any reasonable adjustments as necessary
- To comply with payroll, auto-enrolment and RTI responsibilities

The organisation may collect this information in a variety of ways, for example from application forms, CVs or resumes, obtained from your passport or other identity documents such as your driving licence, from forms completed by you at the start of or during employment (such as pensions benefit nomination forms), from correspondence with you or through interviews, meetings or other assessments.

This personal data might be provided to us by you, or someone else (such as a former employer's reference, information from background check providers including criminal records checks permitted by law) or it could be created by us.

Your personal data will be stored in a range of different places including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

Throughout your employment we will collect data and add to your personnel file, i.e., appraisal paperwork, communications, absence information and changes to personnel data.

Special categories of personal data

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to job applicants with disabilities).

Where the organisation processes other special categories of personal data such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. This is to carry out its obligations and exercise specific rights in relation to employment.

Automated decision-making

Employment decisions are not based solely on automated decision-making.

How do we lawfully use your data?

We need to know your personal, sensitive and confidential data in order to employ you. Under the UK GDPR, we will be lawfully using your information in accordance with:

- Article 6, (b) Necessary for performance of/entering into contract with you
- Article 9(2) (b) Necessary for controller to fulfil employment rights or obligations in employment

This notice applies to the personal data of our employees and the data you have given us about your carers/family members.

How do we maintain the confidentiality of your record?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018 (incorporating the UK GDPR at Part 2, Chapter 2)
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- NHS Codes of Confidentiality, Information Security and Records Management

We will only ever use or pass on information about you to others who have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e., life or death situations) or where the law requires information to be passed on.

Our policy is to respect the privacy of our candidates and to maintain compliance with the UK GDPR and all UK specific Data Protection Requirements. Our policy is to ensure all personal data will be protected.

All employees and sub-contractors engaged by this organisation are asked to sign a confidentiality agreement. The organisation will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for the organisation, an appropriate contract will be established for the processing of your information.

In certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the data protection officer in writing if you wish to withdraw your consent. In some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Where do we store your information electronically?

All the personal data we process is processed by our organisation in the UK. However, for the purposes of IT hosting and maintenance this information may be located on servers within the European Union.
No third parties have access to your personal data unless the law allows them to do so, and appropriate safeguards have been put in place.
We have a data protection regime in place to oversee the effective and secure processing of your personal and or special category (sensitive, confidential) data.

Artificial Intelligence (AI)

Prior to using AI, a full data protection impact assessment (DPIA) has been compiled, and any AI use will comply with the strict UK data protection laws that also include UK GDPR. The lawful basis to process your personal data does not change because we use AI.

For further information on how AI may be used, refer to the organisation's Privacy Notice – Artificial Intelligence.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations:

- Primary Care Networks
- Integrated Care Systems/Integrated Care Boards
- NHS Commissioning Support Units
- NHS England (NHSE)

- Local authorities
- CQC
- Other ‘data processors’ which you will be informed of

Sharing your personal data

Your information may be shared internally including with members of the HR and recruitment team (including payroll), your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

Sometimes we might share your personal data with other organisations within our group or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests, for example to obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service, payroll, the provision of benefits and the provision of occupational health services. We use Smartclinc, Teamnet, Glen Payroll, Mayflower Disclosure Services, Gov.uk DBS Update Service, National Workforce Tool and the ICB.

The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation will not transfer your data to countries outside the European Economic Area.

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

We may also use external companies to process personal information such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged by this organisation are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for the organisation, an appropriate contract will be established for the processing of your information.

Who is the data controller?

This organisation is registered as a data controller under the Data Protection Act 2018. Our registration number is Z6863570 and our registration can be viewed upon the ICO website at https://ico.org.uk/esdwebpages/search. This means we are responsible for handling your personal and healthcare information and collecting and storing it appropriately.

We may also process your information for a particular purpose and therefore we may also be data processors. The purposes for which we use your information are set out in this privacy notice.

How long do we keep your personal information?

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records Management Code of Practice for health and social care and national archives requirements.

More information on records retention can be found online at: NHSE – Records Management Code of Practice.

How can you access, amend or move the personal data that you have given to us?

Even if we already hold your personal data, you still have various rights in relation to it. For further information about this, contact the Kelly Houseman the Practice Manager. We will seek to deal with your request without undue delay and in any event in accordance with the requirements of any applicable laws.

Please note that we may keep a record of your communications to help us resolve any issues which you raise.

- **Right to object**:

  If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply.

- **Right to withdraw consent**:

  Where we have obtained your consent to process your personal data for certain activities (for example for a research project), or consent to market to you, you may withdraw your consent at any time.

- **Right to erasure**:

  In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will generally

assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data is collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

- **Right of data portability**:

  If you wish, you have the right to transfer your data from us to another data controller.

Your rights as an employee

Data Subject Access Requests (DSAR): You have a right under the data protection legislation to request access to view or to obtain copies of what information this organisation holds about you and to have it amended should it be inaccurate. To request this, you need to do the following:

- Your request should be made to Kelly Houseman, Practice Manager at Kelly.Houseman@nhs.net

- There is no charge to have a copy of the information held about you. However, we may, in some limited and exceptional circumstances, have to make an administrative charge for any extra copies if the information requested is excessive, complex or repetitive

- We are required to provide you with information within one month. We would ask therefore that any requests you make are in writing and it is made clear to us what and how much information you require

- You will need to give adequate information (for example full name, address, date of birth and details of your request) so that your identity can be verified, and your records located

What should you do if your personal information changes?

You should tell us so that we can update our records. Please contact the Practice Manager, Kelly Houseman as soon as any of your details change, this is especially important for changes of address or contact details (such as your mobile phone number). Eve Hill Medical Practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

What to do if you have any questions

Should you have any questions about this privacy policy or the information we hold about you, you can:

- Contact the organisation via email at bcicb.evehill@nhs.net
- Write to the data protection officer Michelle K Norcup at bcicb.dpo@nhs.net
- Ask to speak to the Practice Manager Kelly Houseman or their deputy Karen Webb

Objections or complaints

In the unlikely event that you are unhappy with any element of our data-processing methods, do please contact the Practice Manager at this organisation in the first instance. If you feel that we have not addressed your concern appropriately, you have the right to lodge a complaint with the ICO. For further details, visit https://ico.org.uk/for-the-public/ and select “Make a complaint” or telephone: 0303 123 1113.

The ICO is the regulator for the UK GDPR and offers independent advice and guidance on the law and personal data including your rights and how to access your personal information.

Changes to our privacy policy

We regularly review our employee privacy policy, and any updates will be published to reflect the changes. This policy is to be reviewed March 2027.