

j

ELSENHAM SURGERY

EMPLOYEE PRIVACY NOTICE

Data Controller: Karen Greaves Practice Manager

Data Protection Officer: Jane Marley (WECCG)

Caldicott Guardian – Karen Greaves

The practice collects and processes personal data relating its employees to manage the employment relationship. The practice is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the practice collect?

The practice collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the practice;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the practice needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.
- Contact information for your next of kin – to be contacted in an emergency.

The practice collects this information in a variety of ways, such as:

- Application forms:

- CVs or resumes;
- Copies of your passport other identity documents;
- Information collected through interviews or other forms of assessment;
- Forms completed by you at the start of or during employment;
- From correspondence with you;
- Through meetings or other assessments.

The practice will also collect personal data about you from third parties, such as:

- References supplied by former employers;
- Information from employment background check providers and information from criminal records checks;
- The practice may seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including:

- Your application record;
- HR management systems;
- IT systems (including email).
- With selected third parties to process our legal obligations as your employer.

Why does the practice process personal data?

The practice needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. It needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the practice needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. It is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the practice has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the practice to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;

- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the practice complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where the practice relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

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 employees with disabilities and for health and safety purposes). Where the practice processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

Who has access to data?

Your information will be shared internally. This includes:

- Your manager/supervisor
- The Partners
- Payroll
- IT and Smartcard
- Emis
- Peninsula
- Equip and other trainers.
- Intradoc
- DBS Checking Services
- E-Learning - Bluestream
- Previous Employers – with regard to references.
- The Practice Website and publications.
- CCG and NHS England as appropriate.
- BDO accountants

The practice shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

The practice is obliged to seek information about criminal convictions and offences in line with NHS Employers guidelines on criminal records checks, which you can read at:

<http://www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check>

The practice 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 practice also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services. The practice shares your data with the third-party agencies listed above in order to fulfil its legal obligations to you as your employer.

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

How does the practice protect data?

The practice takes the security of your data seriously. Internal policies and controls are in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. All HR and Data Protection Policies can be found on Intradoc.

Where the practice engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and practice measures to ensure the security of data.

For how long does the practice keep data?

The practice will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment is 7 years.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the practice to change incorrect or incomplete data;
- require the practice to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the practice is relying on its legitimate interests as the legal ground for processing; and
- ask the practice to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the practice's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact Karen Greaves Practice Manager. You can make a subject access request by completing the practice's form for making a subject access request. The SAR will be processed within 1 month and is free of charge.

If you have a complaint about how your data is processed that cannot be resolved with the Practice, you have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office at www.ico.org.uk.

What if you do not provide personal data?

You have some obligations under your employment contract to provide the practice with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the practice with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the practice to enter a contract of employment with you. If you do not provide other information, this will hinder the practice's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based on automated decision-making.

Our Website

Privacy Notice only applies to the practice. Link to any other website, please read their Privacy Notice. WE TAKE NO RESPONSIBILITY for content of other website. The practice website uses cookies. For more information on which cookies our website uses and how they are used , please go to:

<https://elsenhamsurgery.secure-gpsite.nhs.uk/index.php?disclaimer=1#cookies>

Cookies

Cookies are small text files located in browser directories. When you visit a site that uses cookies for the first time, a cookie is downloaded onto your PC. The next time you visit that site, your PC checks to see if it has a cookie that is relevant (that is, one containing the site name) and sends the information contained in that cookie back to the site. The site then 'knows' that you have been there before, and in some cases, tailors what pops up on screen to take account of that fact.

Are they good or bad?

They are beneficial because they can record preferences and store data (e.g. what's in your online shopping cart). They can make sites easier to navigate and create a more personal browsing experience. The negative aspect of cookies is that information about you, however benign, is collected and stored by a website and can be used to market services to you or shared with a third party who may wish to do the same.

WiFi

Elsenham Surgery provides free publicly accessible WiFi. The service has been kindly provided by West Essex CCG. Use of the WiFi service is conditional, and by making use of the WiFi provided, you are indicating your agreement to the terms. The practice has no access to data held or control over WI-FI and password provided where terms and conditions apply.