

General Practice Privacy Notice

Protecting Your Data

Introduction

This staff privacy notice explains in detail why we use your personal data which we, the GP practice (Data Controller), collects and processes about you. A Data Controller determines how the data will be processed and used and others who we share this data with. We are legally responsible for ensuring that all personal data that we hold and use is done so in a way that meets the data protection principles under the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018. This notice also explains how we handle that data and keep it safe.

Caldicott Guardian

The GP Practice has a Caldicott Guardian. A Caldicott Guardian is a senior person within a health or social care organisation, preferably a health professional, who makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. The Caldicott Guardian for the GP practice is:

Dr Khine Kyaw
Cedar Cross Medical Centre
Whiston PCRC
Old Colliery Road
Whiston
L35 3SX

Cmicb-kn.cedarcrossmc@nhs.net

Data Protection Officer (DPO)

Under UK GDPR all public bodies must nominate a Data Protection Officer. The DPO is responsible for advising on compliance, training and awareness and is the main point of contact with the Information Commissioner's Office (ICO). The DPO for the practice is:

Information Governance Team
Mid Mersey Digital Alliance
Jubilee Court
Academy Site
Waterside
St Helens
WA9 1TT

Or via DPO@midmerseyda.nhs.uk

We will continually review and update this privacy notice to reflect changes in our services and to comply with changes in the law. When such changes occur, we will revise the last updated date as documented in the version status in the header of this document.

Definition of Data Types

We use the following types of information / data:

Personal Data

This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under UK GDPR, this now includes location data and online identifiers.

Special categories of data (previously known as sensitive data)

This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under UK GDPR, this now includes biometric data and genetic data.

Personal Confidential Data (PCD)

This term came from the [Caldicott review](#) undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Pseudonymised Data or Coded Data

Individual-level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity. When data has been pseudonymised it still retains a level of detail in the replaced data by use of a key / code or pseudonym that should allow tracking back of the data to its original state.

Anonymised Data

This is data about individuals but with all identifying details removed. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

Aggregated Data

This is statistical information about multiple individuals that has been combined to show general trends or values without identifying individuals within the data.

Who we are

Cedar Cross Medical Centre employs more than nine staff and operate from Whiston Primary Care Resource Centre

Our Practice is registered with the Information Commissioner's Office (ICO) to process personal and special categories of information under the Data Protection Act 2018 and our registration number is **Z4849881**

For further information please refer to the 'About US' page on our website:
www.cedarcrossmedicalcentre.co.uk

Why we collect personal information about you

The Practice collects stores and processes personal information about prospective, current and former staff to ensure compliance with legal and/or industry requirements.

What is our legal basis for processing your personal information?

Processing of employee personal information is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller (the Practice) or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

The Practice does not require explicit consent of staff or workers to process their personal data if the purpose falls within the legal basis detailed above.

For further information on this legislation please visit: <http://www.legislation.gov.uk/>

What personal information do we need to collect about you and how do we obtain it?

Personal information about you will largely be collected directly from you during your recruitment and employment. Personal information may also be collected from healthcare professionals in certain circumstances, through national checks such as DBS etc.

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

- Personal demographics (including gender, race, ethnicity, sexual orientation, religion)
- Contact details such as names, addresses, telephone numbers and emergency contact(s)
- Employment records (including professional membership, references and proof of eligibility to work in the UK and security checks)
- Bank details
- Pension details

- Occupational health information (medical information including physical health or mental condition)
- Information relating to health and safety
- Trade union membership
- Practice Directors / membership
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Employment Tribunal applications, complaints, accidents, and incident details

What do we do with your personal information/ What we may do with your personal information?

Your personal information is processed for the purposes of:

- Staff administration and management (including payroll and performance)
- Pensions administration
- Business management and planning
- Accounting and Auditing
- Accounts and records
- Education
- Health administration and services
- Information and databank administration
- Crime prevention and prosecution of offenders
- Sharing and matching of personal information for national fraud initiative

Who do we share your personal information with and why?

We will not routinely disclose any information about you without your express permission. However, in order to enable effective staff administration and comply with our obligations as your employer, we will share the information which you provide during the course of your employment (including the recruitment process) with the NHS Business Services Authority for maintaining your employment records.

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

Where possible, we will always look to anonymise/ pseudonymise your personal information so as to protect confidentiality, unless there is a legal basis that permits us to use it, and will only ever use/ share the minimum information necessary. However, there are occasions where the Practice is required by law to share information provided to us with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

For any request to transfer your data internationally outside the UK/EU we will make sure that an adequate level of protection can be satisfied before the transfer.

There are a number of circumstances where we must or can share information about you to comply or manage with:

- Disciplinary/ investigation processes; including referrals to Professional Bodies, e.g. NMC and GMC;
- Legislative and/or statutory requirements;
- A Court Orders which may have been imposed on us;
- NHS Counter Fraud requirements;
- Request for information from the police and other law enforcement agencies for the prevention and detection of crime and/or fraud if the crime is of a serious nature.

How we maintain your records

Your personal information is held in both paper and electronic forms for specified periods of time as set out in the NHS Records Management 2021 and National Archives Requirements. We hold and process your information in accordance with UK GDPR & the Data Protection Act 2018.

In addition, everyone working for the NHS must comply with the Common Law Duty of Confidentiality and various national and professional standards and requirements.

We have a duty to:

- Maintain full and accurate records of your information.
- Keep records about you confidential and secure.
- Provide information in a format that is accessible to you.

Use of Email - The Practice may provide the option to communicate with staff via email. Please be aware that the Practice cannot guarantee the security of this information whilst in transit, and by requesting this service you are accepting this risk.

How we protect your personal data

We will use the information in a manner that conforms to the UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018. The information you provide will be subject to rigorous measures and procedures to make sure it can't be seen, accessed or disclosed to any inappropriate persons. We have an Information Governance Framework that explains the approach within the GP practice, our commitments and responsibilities to your privacy and cover a range of information and technology security areas.

Our IT Services provider, Mid Mersey Digital Alliance, regularly monitor our system for potential vulnerabilities and attacks and look to always ensure security is strengthened.

All our staff have received up to date data security and protection training. They are obliged in their employment contracts to uphold confidentiality, and may face disciplinary procedures if they do not do so. We have incident reporting and management processes in place for reporting any data breaches or incidents. We learn from such events to help prevent further issues and inform patients of breaches when required.

How long do we keep your personal data?

Whenever we collect or process your data, we will only keep it for as long as is necessary for the purpose it was collected. For a GP practice, we comply with the [Records Management NHS Code of Practice 2021](#) . Following this time, the records are securely destroyed if stored on paper, deleted on the electronic health record system or archived for research purposes where this applies.

Destruction

This will only happen following a review of the information at the end of its retention period. Where data has been identified for disposal we have the following responsibilities:

- to ensure that information held in manual form is destroyed using a cross cut shredder or contracted to a reputable confidential waste company SHRED IT that complies with European Standard EN15713 and obtain certificates of destruction.
- to ensure that electronic storage media used to hold or process information are destroyed or overwritten to national standards.

What are your rights over your personal data?

You have the following rights over your data we hold:

- Subject Access Rights
You can request access to and or copies of personal data the practice holds about you, free of charge (subject to exemptions) and provided to you within 1 calendar month. We request that you provide us with adequate information in writing to process your request such as full name, address, date of birth, NHS number and details of your request and documents to verify your identity so we can process the request efficiently. On processing a request, there may be occasions when information may be withheld if the practice believes that releasing the information to you could cause serious harm to your physical or mental health. Information may also be withheld if another person (i.e. third party) is identified in the record, and they do not want their information disclosed to you.

To request a copy or request access to information we hold about you and / or to request information to be corrected if it is inaccurate, please contact:

Practice Manager

cmicb-kn.cedarcrossmc@nhs.net

Cedar Cross Medical Centre
Whiston PCRC
Old Colliery Road
Whiston
L35 3SX

- Right to rectification

The correction of personal data when incorrect, out of date or incomplete which must be acted upon within 1 calendar month of receipt of such request. Please ensure the GP practice has the correct contact details for you.

- Right to withdraw consent
If we have your explicit consent for any processing we do, you have the right to withdraw that consent at any time.
- Right to Erasure ('be forgotten')
If we obtain consent for any processing we do, you have the right to have that data deleted / erased. Please note this does not apply to health records.
- Right to Data Portability
If we obtain consent for any processing we do, you have the right to have data provided to you in a commonly used and machine readable format such as excel spreadsheet, csv file.
- Right to object to processing
You have the right to object to processing however please note if we can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue.
- Right to restriction of processing
This right enables individuals to suspend the processing of personal information, for example, if you want to establish its accuracy or the reason for processing it.

Complaints / Contacting the Regulator

If you feel that your data has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, please contact our Data Protection Officer / Practice Manager at the following contact details:

Email us at: cmicb-kn.cedarcrossmc@nhs.net

Or write to us at: Cedar Cross Medical Centre, Whiston PCRC, Old Colliery Road, Whiston, L35 3SX

If you are not happy with our responses and wish to take your complaint to an independent body, you have the right to lodge a complaint with the Information Commissioner's Office.

You can contact them by calling 0303 123 1133

Or go online to www.ico.org.uk/concerns (opens in a new window, please note we can't be responsible for the content of external websites)

Further Information / Contact Us

We hope that the Staff Privacy Notice has been helpful in setting out the way we handle your personal data and your rights to control it. Should you have any questions / or would like

further information, please contact either the practices Caldicott Guardian / Data Protection Officer / Practice Manager at the following contact details:

Email us at: cmicb-kn.cedarcrossmc@nhs.net

Or write to us at: Cedar Cross Medical Centre, Whiston PCRC, Old Colliery Road, Whiston, L35 3SX