Primary Integrated Community Services Ltd

Primary Integrated Community Services Ltd (PICS)

This document applies to all associated PICS GP Practices, Services and employees.

PICS Patient Privacy Notice

Document Control

A. Confidentiality and Equality Notice

This document and the information contained therein is the property of Primary Integrated Community Services Ltd.

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Primary Integrated Community Services Ltd.

All PICS policies are tested using the PICS Equality Impact Assessment tool at the time of issue and renewed with every substantial update to the policy. A PICS policy will only be published and enforced once a policy is deemed to have an overall positive or neutral impact on all protected characteristics. The EIA can be found at the back of this policy.

B. Document Details

Classification:	Information Governance
Author and Role:	Chelsi Wightman, Information Governance Lead
Champion:	Data Protection Officer
Organisation:	Primary Integrated Community Services Ltd
Version Number:	1.0
Last Ratification Date:	October 2025
Review Date:	October 2026
Current Document Approved By:	PICS Policy Ratification Committee
Scope:	Applicable to all PICS employees, volunteers, contractors and people who are working for the Organisation.
Issue Date:	September 2025
Equality Impact Assessment:	completed and neutral

C. Document Revision and Approval History

Version	Date	Version Created By:	Comments and details of changes made

1.0	September 2025	Chelsi Wightman (adapted from PCIG)	Policy re-write. Inclusion on SystmConnect and AI.
1.1	October 2025	Chelsi Wightman	Added Notts Care Record information to 'Data Sharing and Third Parties'

D. **Policy Summary**

This Privacy Notice explains how PICS collects, uses, shares, and protects your personal data. It covers data processed for direct care, NHS services, and organisational functions. We follow UKGDPR and NHS standards.

E. **Related Policies and Procedures**

PICS Children/Candidate/Employee Privacy Notice
PICS Confidentiality and Data Protection Policy
PICS GDPR Policies
PICS AI Implementation Policy
PICS Access to Online Services (Practices) Policy

Introduction

This Privacy Notice explains how Primary Integrated Community Services Ltd ("PICS") and it's associated GP Practices collect, uses, and protects your personal data. It applies to all personal information processed by or on behalf of PICS, including our associated GP Practices and services.

We are committed to safeguarding your privacy and ensuring that your data is handled lawfully, transparently, and securely.

This Notice covers:

- Who we are and how we use your information
- Information about our Data Protection Officer
- What kinds of personal information we hold and process
- The legal grounds for processing your personal information (including when we share it with others)
- What to do if your personal information changes
- How long your personal information is retained
- Your rights under Data Protection laws

PICS is the data controller for your personal information under the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018 (DPA 2018). These laws came into effect on 25 May 2018 and were retained in UK law following the UK's exit from the EU on 1 January 2021.

Your privacy is important to us, and we are committed to protecting your data privacy rights.

Your Data and How we Use It

Who Controls Your Data

Primary Integrated Community Services Ltd (PICS) is the Data Controller for the personal information we collect and process. This means we are responsible for ensuring your data is handled lawfully, securely, and in accordance with data protection legislation. If you are registered at a PICS GP Practice (Hama Medical Centre, Meden Medical Services, Saxon Cross Surgery or Whyburn Medical Practice) then these GP Practices will be the Data Controller for you information and adhere to all points in this policy.

What Information We Collect

We collect and process the following types of personal data:

- Basic personal data: Name, address, date of birth, contact details (email, mobile number), and location-based information.
- Special category data: Health information, ethnicity, religious beliefs (where relevant in a healthcare setting), and sex life information linked to your care.
- Third-party data: Information received from other healthcare providers, social care services, or organisations involved in your care.

Why We Need Your Information

We collect your data to:

- Provide safe, effective, and personalised healthcare services
- Maintain accurate and up-to-date medical records.
- Support clinical decision-making and continuity of care.
- Fulfil legal and contractual obligations under NHS service delivery.

Your records may include:

- Contact details and emergency contacts.
- Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments.
- Notes and reports about your health.
- Details of treatment, investigations, and referrals, including results of investigations such as laboratory tests, x-rays etc.
- Information from other health professionals or caregivers.
- Notes and reports about your health.

These records may be held electronically, on paper, or both. We use secure systems and robust working practices to protect your information.

How We Use Your Information

Your data may be used for:

- Direct care and treatment, including telephone and video consultations.
- Contacting you about appointments, test results, or health services.
- Clinical audits to monitor and improve service quality.
- Supporting public health initiatives and NHS service planning.
- Legal obligations, such as safeguarding, court orders, or law enforcement requests.
- De-identified data analysis to improve population health outcomes.

We will never share your personal information with anyone who does not need it or who does not have a legal right to access it, unless you give us explicit consent.

Legal Basis for Processing Your Data

We process your data under the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018, using the following legal bases:

- Article 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Article 9(2)(h) – Processing is necessary for preventive or occupational medicine, medical diagnosis, provision of health or social care, or management of health systems.
- Consent: When you have given us consent
- Vital Interest: If you are incapable of giving consent, and we have to use your information to protect your vital interests (e.g. if you have had an accident and you need emergency treatment)
- Defending a claim: If we need your information to defend a legal claim against us by you, or by another party

These legal bases apply to data about patients, carers, and family members where relevant to your care.

The law states that personal information about your health falls into a special category of information because it is very sensitive. Reasons that may entitle us to use and process your information may be as follows:

Use of Artificial Intelligence

Artificial Intelligence (AI) refers to technologies that perform tasks typically requiring human intelligence, such as understanding language, recognising patterns, or making predictions. PICS uses AI tools to support both clinical and non-clinical functions, always under strict governance and human oversight.

How We Use AI

We may use AI in the following ways:

- Clinical support: Assisting clinicians with decision-making, triage, diagnostics, and summarising clinical notes.
- Operational efficiency: Automating administrative tasks such as appointment scheduling, summarising meeting notes, and generating reports.
- Population health: Analysing anonymised data to identify trends and improve service delivery.

AI tools may be standalone applications or embedded within other systems (e.g. clinical platforms, communication tools). Examples include Microsoft Co-Pilot and Heidi AI, used in a controlled and secure manner.

Governance and Oversight

Before AI can be used a Data Protection Impact Assessment is completed and approved by a Third Party Data Protection Officer. AI is used as a support tool, not a decision-maker. All outputs generated by AI are reviewed and validated by qualified staff. We recognise the risks associated with AI, including:

- Incorrect outputs ("AI hallucinations")
- Bias in training data
- Vulnerability to manipulation ("prompt injection" or "data poisoning")

To mitigate these risks:

- Each AI use case undergoes a risk assessment and approval process.
- Staff receive training on responsible AI use.
- Only authorised personnel access AI-generated content.
- We maintain accountability and ownership of all decisions made using AI tools.

Lawful Basis for AI Use

We process data using AI under the same lawful bases as other data processing activities:

- **Article 6(1)(e)** – Public task or official authority
- **Article 9(2)(h)** – Provision of health or social care

Where AI is used for purposes beyond direct care (e.g. service planning or research), data is anonymised or pseudonymised in accordance with UKGDPR and NHS standards

Transparency and Your Rights

We are committed to transparency in how AI is used. You will not be subject to decisions made solely by automated systems. If AI is used in your care, it will be to support—not replace—clinical judgement.

You have the right to:

- Be informed about how your data is used in AI systems
- Object to the use of your data in non-direct care AI applications
- Request further information from our Data Protection Officer or Information Governance Lead

Data Sharing and Third Parties

Who We Share Your Information With

To deliver safe, effective, and coordinated care, PICS and it's GP Practices may share your personal data with authorised third parties. This is always done under strict legal and contractual safeguards.

We may share your information with:

- NHS Trusts and Foundation Trusts
- GP Practices and Primary Care Networks (PCNs)
- Integrated Care Boards (ICBs) and NHS England
- Community and mental health services
- Social care providers and local authorities
- Care Homes and Hospices
- Pharmacies, optometrists, dentists
- Ambulance services and NHS 111
- Voluntary and private sector providers involved in your care
- Safeguarding teams, Multi-Agency Safeguarding Hubs (MASH)
- Law enforcement and judicial services including Coroners and Medical Examiners (where legally required)
- General Medical Council
- Education services (where relevant to care provision)
- Research organisations (with appropriate approvals and safeguards)

We will only share the minimum necessary information required for the purpose, and only with organisations that have a lawful basis to process your data. We will not provide your information to any other third parties without your permission unless there are exceptional circumstances, such as, if the health and safety of you and others is at risk or if the law requires us to pass on information.

Third-Party Processors

We also work with carefully selected third-party service providers who support our operations. These providers may process data on our behalf under strict contractual agreements that ensure:

- Data is kept secure and confidential
- Information is only used in accordance with our instructions
- Providers comply with UK data protection laws

Examples of third-party processors include:

- IT system providers and support services
- Electronic health record and appointment booking platforms
- Document management and scanning services
- Secure messaging and communication platforms
- Payment providers (e.g. for travel vaccinations or private services)
- Delivery services (e.g. for medication)

A full list of third-party processors is available on request from our Information Governance Lead and IT and Estates Lead.

Legal Basis for Sharing Data

We share data under the following legal bases:

- Article 6(1)(e) – Public task or official authority
- Article 9(2)(h) – Health or social care provision
- Article 9(2)(b) – Employment and social protection law (e.g. safeguarding)
- Article 9(2)(g) – Substantial public interest (e.g. public health, safeguarding)
- Article 9(2)(j) – Scientific or historical research purposes (with safeguards)

Where required, we will seek your explicit consent before sharing identifiable data for non-care purposes, such as research or service evaluation.

Safeguards and Accountability

All data sharing is subject to:

- Role-based access controls
- Audit trails and monitoring
- Data Sharing Agreements and Framework Contracts
- Professional codes of confidentiality
- Compliance with the National Data Opt-Out policy

We will never sell your data or share it for marketing purposes.

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from several sources including NHS Trusts and from this GP Practice. The identifying parts of your data are removed, analysis of your data is undertaken, and a risk score is then determined. This is then provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way in most circumstances, please contact the practice for further information about opt out.

Individual Risk Management at a GP practice level however is deemed to be part of your individual healthcare and is covered by our legal powers above.

NHS App

We use the NHS Account Messaging Service provided by NHS England to send you messages relating to your health and care. You need to be an NHS App user to receive these messages. Further information about the service can be found at the ***privacy notice for the NHS App*** managed by NHS England.

Research

Clinical Practice Research Datalink (CPRD) collects de-identified patient data from a network of GP practices across the UK. Primary care data are linked to a range of other health related data to provide a longitudinal, representative UK population health dataset. You can opt out of your information being used for research purposes at any time (see below), full details can be found here: -

https://cprd.com/transparency-information

GP Connect

PICS and it's associated GP Practices have reviewed the National Data Sharing Arrangement (NDSA) for GP connect. GP Connect helps clinicians gain access to GP patient records during interactions away from a patient's registered practice and makes their medical information available to appropriate health and social care professionals when and where they need it, to support the patient's direct care.

From a privacy, confidentiality and data protection perspective, GP Connect provides a method of secure information transfer and reduces the need to use less secure or less efficient methods of transferring information, such as email or telephone.

Key points:

- GP Connect can only be used for direct care purposes.
- Individuals can opt out of their GP patient record being shared via GP Connect by contacting their GP practice.
- Access to GP Connect is governed by role-based access control (RBAC) and organisational controls; only people who need to see the GP patient record for a patient's direct care should be able to see it
- All systems that allow the use of GP Connect must undergo a robust compliance process and the organisations involved must sign a connection agreement holding them to high standards of information security.

GP Connect products can help health and social care professionals share, view or act on information that could be required for a patient's direct care, but they would otherwise have difficulty accessing easily (for example if they are using different IT systems).

Organisations can have access to relevant information in GP patient records to provide direct care to patients only.

Type of organisations that use GP Connect

Examples of organisations that may wish to use GP connect to view GP patient records include:

- GP Practices: Including surgeries where patients are not registered (e.g. when away from home)
- GP Hubs, PCNs, ICSs: Collaborative networks and partnerships
- Hospitals and Secondary Care: Including A&E and surgical services
- Community Services: Healthcare professionals providing local care
- Ambulance Trusts: For emergency access to patient records
- Acute and Emergency Care Providers
- NHS 111
- Pharmacies
- Optometrists
- Dentists
- Mental Health Trusts
- Hospices
- Adult and Children's Social Care Services
- Care and Nursing Homes
- Shared Care Record Systems: Local integrated data platforms

All access to your GP patient record is stored within an audit trail at your GP practice and within the organisation that information has been shared with.

If patients do not wish their information to be shared using GP Connect, they can opt out by contacting their GP practice.

Nottingham and Nottinghamshire Ecosystems Platform and Notts Care Record

The Nottingham and Nottinghamshire Ecosystems Platform and Notts Care Record is a shared system that allows healthcare staff within the Nottingham and Nottinghamshire health and social care community to appropriately access the most up-to-date and correct information about patients involved in their care, to deliver the best possible care.

To make sure you get the best care doctors, nurses and the team of health and care staff caring for you keep records about your health and any care or treatment you may receive from the NHS and Social Care. These records help to make sure that you receive the best possible care. These may be written down in your paper records or held on a computer. They may include:

- Basic details about you such as name, address, date of birth, next of kin, etc.
- Contact we have had with you such as appointments or clinic visits,
- Notes and reports about your health, treatment and care,
- Results of x-rays, scans and laboratory tests,

- Relevant information from people who care for you and know you well such as health professionals and relatives.

Always check that your details are correct when you visit us and please tell us of any changes as soon as possible.

Your records are used to manage and deliver the care you receive to make sure that:

- The doctors, nurses and other healthcare members of staff involved in your care have correct and up to date information, to look at your health and decide on the right care for you,
- Health and care staff have the information they need to be able to look at and improve the quality and type of care you receive,
- Your concerns and worries can be properly investigated if a complaint is raised,
- The right information is available if you see another doctor, or are referred to a specialist or another part of the NHS and Social Care.

The Notts Care Record is sub-processed by Interweave:
https://www.interweavedigital.com/

If you would like any further information, or would like to discuss this further, please contact us using the details provided in Contact Information.

Your Rights

Under the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018, you have a number of rights regarding the personal data we hold about you. These rights are designed to give you control over how your information is used and to ensure transparency in our data processing activities.

You can exercise any of these rights by contacting our Information Governance Lead or Data Protection Officer. We aim to respond to all requests within one calendar month, although this may be extended in complex cases.

Right to Access

You have the right to request access to the personal data we hold about you. This includes:

- Viewing your medical records
- Receiving a copy of your data
- Understanding how your data is being used

There is no charge for this service, and you will need to provide sufficient information to verify your identity.

You may be able to access your information online, please contact the Service directly to discuss this option.

Right to Rectification

If any of the information we hold about you is inaccurate or incomplete, you have the right to request that it be corrected.

Right to Erasure ("Right to be Forgotten")

In certain circumstances, you may request that we delete your personal data. This applies when:

- The data is no longer necessary for the purpose it was collected
- You withdraw consent (where consent was the legal basis)
- The data has been unlawfully processed

Please note: We may need to retain some information to comply with legal obligations or for public health reasons.

Right to Restrict Processing

You can ask us to restrict the use of your data if:

- You contest its accuracy
- You object to its processing
- You believe it has been unlawfully processed but do not want it erased

Right to Object

You have the right to object to the processing of your data where we rely on public interest or legitimate interest as the legal basis. This includes:

- Direct marketing (if applicable)
- Data used for research or statistical purposes

We will consider your objection and only continue processing if we can demonstrate compelling legitimate grounds.

Right to Data Portability

You can request that your data be transferred to another provider. This applies to data you have provided to us directly and where processing is based on consent or contract.

We will support this through GP-to-GP electronic transfers and provision of paper records where necessary.

Right to Withdraw Consent

Where we rely on your consent to process your data (e.g. for research participation or non-clinical communications), you have the right to withdraw that consent at any time.

Right to Complain

If you are unhappy with how your data is being handled, you can raise a concern with our Information Governance Lead or our Data Protection Officer. If you remain dissatisfied, you have the right to lodge a complaint with the UK's supervisory authority:

Information Commissioner's Office (ICO)
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Tel: 0303 123 1113
Website: https://ico.org.uk

National Opt-Out Facility

The NHS has a National Data Opt-Out which allows patients to choose whether their confidential patient information is used for purposes beyond their individual care.

This means you can decide if your health information is shared for research and planning (for example, to improve NHS services or support medical research). Your choice does not affect your care and treatment.

- If you choose to opt out, your confidential patient information will still be used to support your individual care, but it will not be shared for research or planning purposes (unless there is a legal requirement).

- If you do not opt out, your information may be used for these purposes when allowed by law.

We apply the National Data Opt-Out in line with NHS Digital guidance.

There may still be times when your confidential patient information is used: for example, during an epidemic where there might be a risk to you or to other people's health. You can also still consent to take part in a specific research project.

Will choosing this opt-out affect your care and treatment?

No, your confidential patient information will still be used for your individual care. Choosing to opt out will not affect your care and treatment. You will still be invited for screening services, such as screenings for bowel cancer.

To improve health and care services across England, NHS Digital collects patient data from GP practices through the General Practice Data for Planning and Research (GPDPR) programme. This data helps the NHS to:

- Monitor the safety and effectiveness of care
- Plan and commission better services

- Prevent the spread of infectious diseases
- Support health research and innovation
- Inform national policy and public health initiatives

What Data Is Collected

NHS Digital collects structured and coded data from your GP medical record, including:

- Demographic details (e.g. sex, ethnicity, sexual orientation)
- Clinical information (e.g. diagnoses, symptoms, test results, medications, referrals)
- Data about healthcare staff involved in your care

NHS Digital does not collect:

- Your name or full address
- Free-text notes (e.g. consultation summaries)
- Images, letters, or documents
- Data older than 10 years (for certain categories)
- Data restricted by law (e.g. IVF or gender reassignment codes)

How Your Data Is Protected

Before data is shared, it is pseudonymised — meaning identifiable details (like your NHS number or postcode) are replaced with unique codes. NHS Digital can only re-identify this data in specific circumstances and with a valid legal reason.

All data is stored securely within the UK and is never shared with marketing or insurance companies.

What should you do next?

You do not need to do anything if you are happy about how your confidential patient information is used.

You can change your choice at any time by visiting the NHS website: www.nhs.uk/your-nhs-data-matters or by calling 0300 303 5678.

Security and Confidentiality

We are committed to protecting your privacy and ensuring that your personal data is handled securely, ethically, and lawfully at all times.

All personal data is processed in accordance with:

- The Data Protection Act 2018

- The UK General Data Protection Regulation (UKGDPR)
- The Common Law Duty of Confidentiality
- The Human Rights Act 1998
- The Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security, and Records Management
- The Caldicott Principles

Your Responsibilities

Because we are obliged to protect any confidential information, we hold about you and we take this very seriously, it is imperative that you let us know immediately if you change any of your contact details.

We may contact you using SMS texting to your mobile phone if we need to notify you about appointments and other services that we provide to you involving your direct care, therefore you must ensure that we have your up-to-date details. This is to ensure we are sure we are contacting you and not another person. As this is operated on an 'opt out' basis we will assume that you give us permission to contact you via SMS if you have provided us with your mobile telephone number. Please let us know if you wish to opt out of this SMS service. We may also contact you using the email address you have provided to us. Please ensure that we have your up-to-date details.

There may be occasions where authorised research facilities would like you to take part in research. Your contact details may be used to invite you to receive further information about such research opportunities.

Staff Responsibilities

All staff working for or on behalf of PICS, including contractors and volunteers, are required to:

- Complete mandatory data security and protection training
- Sign confidentiality agreements
- Follow internal policies and procedures for data protection and information governance

Failure to comply may result in disciplinary action, including dismissal.

How We Keep Your Data Secure

We use a combination of technical, physical, and organisational measures to protect your data, including:

- Encrypted clinical systems and secure servers
- Role-based access controls and audit trails
- Two-factor authentication and password protection

- Secure email and messaging platforms
- Regular system updates and vulnerability assessments
- Compliance with the NHS Data Security and Protection Toolkit

We also ensure that any external providers (e.g. IT support, scanning services) meet NHS standards for data protection and security.

Confidentiality in Practice

We will only use or share your information when:

- It is necessary for your direct care
- There is a legal requirement or overriding public interest
- You have given explicit consent
- It is required to protect life or prevent serious harm

We follow the principle that "the duty to share information can be as important as the duty to protect confidentiality," as outlined in the Caldicott Review.

Use of De-Identified Data

In some cases, we may use anonymised or pseudonymised data for:

- Service planning and improvement
- Population health management
- Clinical audits and research

This data cannot be used to identify you and is handled in accordance with the ICO's Anonymisation Code of Practice and NHS Digital guidance.

Reporting and Managing Data Breaches

Please see PICS Data Breach Reporting Policy for detailed information. We report all Data Breached to the Data Protection Security Toolkit, and the Information Commissioners Office for review if necessary.

PICS has internal systems for monitoring and investigating and breach or potential breach of patient information.

National Data Opt-Out

The National Data Opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning.

The National Data Opt-out only applies to any disclosure of data for purposes beyond direct care, so having National Data Opt-out will not prevent your GP patient record being shared via GP Connect.

Retention and Disposal

For detailed information on PICS retention and disposal of information and records, please see PICS Retention Policy.

We are required under UK law to retain your personal data for specific periods, depending on the type of information and its purpose. These retention periods are defined by the NHS Records Management Code of Practice for Health and Social Care and the National Archives requirements.

How Long We Keep Your Information

Your records will be retained for the minimum period necessary to fulfil legal, clinical, and operational requirements. This includes:

- Medical records: Retained in accordance with NHS guidance (e.g. GP records are typically kept for 10 years after a patient's death).
- Safeguarding records: Retained for longer periods due to their sensitivity and potential future relevance.
- Administrative records: Retained based on business need and legal obligations.

Where retention periods differ, we follow the most stringent applicable standard.

Secure Disposal of Records

When records are no longer required, they are disposed of securely and in accordance with NHS and legal standards. This includes:

- Paper records: Shredded or incinerated using approved confidential waste services or equipment.
- Electronic records: Permanently deleted using secure data erasure methods.

We ensure that disposal processes are documented, auditable, and carried out by authorised personnel or approved contractors.

Our website

The only website this Privacy Notice applies to is PICS website or the individual GP Practice websites (Hama Medical Centre, Meden Medical Services, Saxon Cross Surgery and Whyburn Medical Practice). If you use a link to any other website from these websites then you will need to read their respective Privacy Notice. We take no responsibility (legal or otherwise) for the content of other websites.

Our websites use Cookies. For more information on which cookies we use and how we use them, please see our Cookies Policy.

CCTV recording

CCTV may be installed at our premises covering both the external area of the building and the internal area excluding consulting rooms. Images are held to improve the personal security of patients and staff whilst on the premises, and for the prevention and detection of crime. The images are recorded onto an integral hard drive of the equipment and are overwritten on a rolling basis. Viewing of these digital images is password protected and controlled by the Site Manager.

Telephone system

Our telephone system records all telephone calls. Recordings are retained for up to three years and are used periodically for the purposes of seeking clarification where there is a dispute as to what was said and for staff training. Access to these recordings is restricted to named senior staff.

Contact Information

PICS Data Protection Officer is Paul Couldrey of PCIG Consulting Limited. Any queries regarding Data Protection issues should be addressed to him at:

PCIG Consulting Limited
7 Westacre Drive
Quarry Bank
Dudley
West Midlands
DY5 2EE
Couldrey@me.com

PICS Information Governance Lead is Chelsi Wightman. Any queries regarding Information Governance or Data Breaches should be addressed to her at:

Primary Integrated Community Services Ltd
Unit H3 Ash Tree Court
Mellors Way
Nottingham Business Park
Nottingham
NG8 6PY
Chelsi.wightman@nhs.net

PICS IT and Estates Manager is Stuart Woolley. Any queries regarding systems and electronic data should be addressed to him at:

Primary Integrated Community Services Ltd
Unit H3 Ash Tree Court
Mellors Way
Nottingham Business Park

Nottingham
NG8 6PY
Stuart.woolley2@nhs.net

Changes to this Notice

We may update this Privacy Notice from time to time to reflect:

- Changes in legislation or regulatory requirements
- Updates to our services or systems
- Improvements in how we communicate with you
- Feedback from patients, staff, or regulators

Any changes will be published on our website and made available at our premises.

Where significant changes are made, we will take reasonable steps to inform you — for example, via email, SMS, or public notices.

We encourage you to review this Privacy Notice periodically to stay informed about how we protect your personal data.

If you have any concerns or questions about changes to this Notice, please contact our Data Protection Officer or Information Governance Lead.