Staff Privacy Notice 2024/25

Staff Information
The purpose of this Privacy Notice is to inform staff employed/contracted by Kent and Medway ICB about the nature and source of any information processed about them, how it will be used, who it will be disclosed to, how we keep it secure and confidential, and staff rights.

For the purposes of this Privacy Notice, 'staff' includes applicants, employees, workers (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience.
The function of completing HR Transactional Services has been outsourced by the ICB to Kent Community Health Foundation Trust (KCHFT).

During the course of these activities the ICB, and KCHFT as a data processor acting on our behalf, will process (obtain, record, hold, use and disclose) personal and special category data (previously known as sensitive data) about our prospective, current and former staff. Personal data is defined as any information relating to a living identified or identifiable natural person who can be identified directly or indirectly from the information. Special Category data is defined as sensitive personal data and incorporates:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs*
- Trade union membership.
- Health data.
- Data regarding an individual's sex life or sexual orientation*.
- Genetic and biometric data used for the purpose of identifying an individual.

For more information on the types of data held please see the types of data handled section below and the data flows table at the end of this document.

We only process your personal and special category data where we have your consent or another legal basis to do so, and where processing can be justified under the UK General Data Protection Regulations / Data Protection Act 2018 (DPA). These include circumstances where the processing is necessary for performance of staff contracts with the ICB or for compliance with any legal obligations that apply to the ICB as your employer.

What laws are relevant to the handling of personal data?
The law determines how organisations can use personal and special category data. The key legislation governing the use of data is listed below:

- The UK General Data Protection Regulations.
- The Data Protection Act 2018.
- The Human Rights Act 1998.
- Freedom of Information Act 2000.
- Computer Misuse Act 1998.
- Audit Commission Act 1998.
- Regulation of Investigatory Powers Act 2000.
- Access to Health Records Act 1990.

The above key legislation stipulates requirements regarding the use of your personal and

special category data; however, the law is primarily set out in the DPA 2018. For the purposes of the DPA, the ICB is the "Controller" (the person or group of people who decide how any why data is processed) of staff information.

Everyone working for the NHS has a legal duty to keep information about you confidential and comply with the Common Law Duty of Confidence. The information we do hold about you, whether in paper or electronic form, is therefore protected from unauthorised access.

What types of personal and/or special categories data do we handle?
In order to carry out activities and obligations as an employer we may process your personal and special category data, such as:

- Contact details such as names, addresses, telephone numbers.
- Emergency contact(s).
- Education and training.
- Employment records (including professional membership, references and proof of eligibility to work in the UK).
- Bank details.
- Pension details.
- Personal demographics (including gender, race, ethnicity, sexual orientation, religion).
- Medical information including physical health or mental health.
- Information relating to health and safety.
- Trade union membership.
- Offences (including alleged offences), criminal proceedings, outcomes and sentences.
- Employment Tribunal applications, complaints, accidents, and incident details.

What is the purpose of processing data?
We only process your personal and special categories data where we have your consent or where the processing can be legally justified under the DPA. These include circumstances where the processing is necessary for the performance of staff contracts with us or for compliance with any legal obligations which apply to the ICB as your employer. These obligations may include (but are not limited to):

- Staff administration (including payroll), including recruitment and selection.
- Pension's administration.
- Business management and planning.
- Accounting and Auditing.
- Accounts and records.
- Crime prevention and prosecution of offenders.
- Education.
- Health administration and services.
- Information and databank administration.
- Sharing and matching of personal information for national fraud initiatives.
- Carrying out of the annual national NHS Staff Survey.
- Administration of the Childcare Voucher Scheme.

Sharing your information
There are a number of reasons why we share information. This can be due to:

- Our obligations to comply with current legislation or regulations.
- Our duty to comply with any Court Order which may be imposed.

Any disclosures of personal and special category data are always made on a case-by-case basis, using the minimum 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 "need to know" or where you have consented to the

disclosure of your personal and special category data to such persons.

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

Payroll Administration (Mersey and West Lancashire NHS Trust)
The payroll of Kent and Medway ICB is managed by Mersey and West Lancashire NHS Trust (MWL). They have been sub-contracted to provide the payroll service by KCHFT. Your personal information will be made available to MWL through ESR (see below) in order to allow them to pay your salary and any associated expenses and to comply with our legal and statutory obligations, including the management of absence monitoring. From time to time we will need to share information with MWL in order to ensure that they deliver the services we require.

Management of Employee Staff Record (ESR)
In order to maintain your employment records, the information which you provide to the ICB during the course of your employment will be held on the national NHS Electronic Staff Record (ESR) system. Your personal and special category data may also be used to fulfil other employer responsibilities, for example, by maintaining appropriate occupational health records, complying with health and safety obligations, carrying out any necessary security checks, and all other employment related matters. In addition, the information held may be used in order to send to you information which is relevant to our relationship with you.

Your information will only be disclosed as required by law or to our appointed agents and/or service providers who may be used for a variety of services; for example, processing of payroll, provision of pensions administration.

IBM, the ICB's Processor who provides ESR, and its partners as service providers will be responsible for maintaining the system. This means that they may occasionally be able to access your staff record, but only to ensure that the ESR works correctly. Even where this happens access will be limited and access is only to allow any problems with the computer system to be fixed as necessary. They will not have the right to use this data for their own purposes and we have contracts in place to ensure that the data is protected and that they only act on our instructions.

Some information from ESR will be transferred to a separate database, known as the Data Warehouse. This will be used by various Government and other bodies. It will allow them to access certain information to generate the reports that they need and are entitled to. These organisations are already accessing this information from the NHS community, and the Data Warehouse is intended to provide a more efficient way of doing this. The bodies using the Data Warehouse may change from time to time. The government may allow further organisations to have access in the future and therefore an exhaustive list cannot be provided, however any organisation having access to your data will have a legal justification for access and will have to comply with the DPA.

National Fraud Initiative
The ICB are required, by law, to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing, or administering public funds, or where undertaking a public function, in order to prevent and detect crime or fraud. Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal and payroll information, and is used for the prevention and detection of fraud

Computerised data matching allows potentially fraudulent claims and payments to be identified. The ICB participate in the Cabinet Office's National Fraud Initiative which is a data matching exercise to assist in the prevention and detection of fraud. We are required

to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise. Once the cabinet office has completed the data matching exercise, any inconsistencies are investigated to determine whether there is or has been fraud taking place. The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 2018. However, data matching by the Cabinet Office is subject to a Code of Practice which can be found on their website.

Staff Survey

The ICB take part in the annual NHS staff survey and staff names, contact details and team details are provided to the IQVIA Solutions UK Ltd for surveys to be distributed. All response reporting is anonymised and no ICB staff are provided with personal results data that would enable individuals to be re-identified.

Giltbyte- expenses system

The ICB use a system called Giltbyte to manage the staff expenses. When a member of staff is employed by the ICB their name, e-mail address and job details are shared with Giltbyte to enable them to create an account. Giltbyte will not access your details, unless requested to do so by yourself or the ICB e.g. to resolve a fault.

Other Bodies

We may also share information with other bodies that inspect and manage public funds. We will not routinely disclose any information about you without your express permission. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation. We may obtain and share personal data with a wide variety of other bodies, which may include, but is not limited to:

- Her Majesty's Revenue and Customs (HMRC) e.g. the HMRC request information on individuals employed by the ICB such as their name, contact details, salary information and payroll information.
- Disclosure and Barring Service – this is managed through Atlantic Data Ltd on behalf of the ICB and staff requiring a DBS check must provide name, contact details (current and previous), date of birth (DOB), National Insurance number, passport and driving license information and job role details.
- Home Office.
- Child Support Agency.
- Central government, government agencies and departments e.g. Job Centre Plus who may require information on whether an individual is employed by the ICB.
- Other local authorities and public bodies.
- Ombudsman and other regulatory authorities.
- Courts/Prisons.
- Financial institutes for e.g. banks and building societies for approved mortgage references.
- Credit Reference Agencies.
- Educational, training and academic bodies.
- Law enforcement agencies including the Police, the Serious Organised Crime Agency.
- Emergency services e.g. The Fire and Rescue Service.
- Auditors e.g. Tiaa.
- Department for Work and Pensions (DWP).
- The Assets Recovery Agency.
- Office of National Statistics (ONS) – The ONS carry out an Annual Survey of Hours and Earnings where they randomly select staff and the ICB is required to provide information under the Statistics of Trade Act 1947. The information provided includes name, National Insurance number, job title, role details, contact details, payroll and salary details and pension details.
- Employers requesting references.

- Dover Counselling Services.
- NEST – the ICB's alternative Pension provider. For those staff not eligible for the NHS pension scheme, they will be auto-enrolled onto the alternative pension scheme provided by NEST. The individual's name, contact details and National Insurance number will be shared with NEST and the individual will be informed that they have been auto-enrolled on the scheme.
- Relatives or guardians of an employee where there is a legal duty to do so

Personal and/or special categories staff information held by the ICB

Finance

Information held for the purposes of payroll audits – held by the ICB Finance Team - includes items of personal data such as your name, your employee number, your pay band and salary. The information held is used to make sure that staff employed by the ICB are on the correct pay band and there are no issues with over or under payments. This information may also be shared with line-managers.

Information will also be required for budget setting and monitoring. Additionally, payroll information will be required for the production of the annual report. If you are in our Childcare Voucher scheme, you will be required to provide your name, contact details, national insurance number and payroll number to Childcare Vouchers. This information will also be accessible to the People and Culture Team.

Recruitment

When someone applies for a job at the ICB they do so through the Trac application tracking system provided by Civica Ltd, the ICBs online recruitment system. Information is collated there and submitted to KCHFT our outsourced recruitment provider for downloading. Following this the data is retained for 400 days and then automatically deleted from the site.

Recruitment information – held by the ICB includes items of personal data such as your name, DOB, address, qualifications and potentially special categories data such as disclosure and barring service self-declaration form details, Occupational Health data and personal references (information held by the People and Culture Team is usually disclosed by yourself or nominated persons providing your reference/s).

Information held is used for the administrative purposes of recruitment and selection. Where we disclose information to a third party, for example where we want to take up a reference or obtain a disclosure from the Disclosure and Barring service, we will not do this without informing you beforehand, unless the disclosure is required by law.

Personal confidential data about unsuccessful candidates will be held for 400 days after the recruitment exercise has been completed. It will then be destroyed or permanently deleted. Once a person has taken up employment with us we will create a record relating to that persons employment on ESR and retain a personal file. Once their employment with us has ended, we will retain the file in accordance with the Records Management Code of Practice 2021.

Further information on individual's rights, including the right to erasure is included below. Please contact the ICB Data Protection Officer for further information.

Workforce diversity data

Workforce data held by the ICB includes details of your protected characteristics as defined by the Equality Act 2010, which are age, disability, gender re-assignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation (disclosed by yourself during the course of your employment). Information held is used for the purpose of monitoring the ICB's equality performance and the diversity of its workforce. This type of information would be stored within ESR.

Training information
The ICB collate data such as names and training courses information (training log) to monitor compliance with mandatory training and to identify training needs via TAPS (staff training system).

Employee Relations
Details of any employee relations cases that have been supported by HR are recorded on ESR, including records of long-term sickness management, capability reviews, suspensions, disciplinary and grievances (provided by you or your line manager during your course of employment). Information held is used for the purposes of supporting and documenting your employment.

Occupational health
Occupational Health services are provided by NHS East Kent Hospitals University Foundation Trust (EKHUFT) Occupational Health Department for the ICB. Data held by the occupational health services provider – includes items of personal and special categories data (disclosed by yourself on your health declaration form or provided by you or your line manager during your course of employment). Information held is used for the purposes of ensuring that you are 'fit for work' and also to ensure you have the appropriate support in the workplace if you have a particular health need..

Personal File
Information held within staff personal files includes items of personal and/or sensitive data (gathered from yourself or other sources during the course of your employment) such as name, address, telephone number, sickness records, records of appraisals, records of capability reviews, HR change forms, details of grievances and disciplinary. Information held is used for the purposes of supporting and documenting your employment.

How information may be used and who it may be disclosed to

- Any personal and special categories data which we obtain and hold will only be used (in an identifiable format) for the purpose for which it was given to us, unless we seek your permission to use it for something else or have another legal basis to do so; and
- If there is a requirement to disclose information we collected for one purpose for a different purpose, generally we would only do this with your explicit consent unless there was another legal basis which permitted disclosure (e.g. statute as in the case of sharing tax information with the tax office, a court order, risk of harm to yourself or another person, or disclosure required in the wider public interest in cases of serious crimes).

When we may publish your information
There are certain circumstances where the ICB is required to publish your information as follows:

- *Conflicts of Interest Register*
- *Conflicts of Interest Breach Register*

All staff are required to complete annual declarations of interests and the ICB is required to publish this information on its website in order to remain open and transparent. Information contained in employee declarations are added to a register, along with details of how the ICB managed any conflicts, and these are uploaded to the ICB's website. Additionally, a separate register detailing breaches of the ICB policy on Conflicts of Interest is also required to be published on the ICB's website.

- *Register of Gifts, Hospitality and Sponsorship*

As with the declarations of interest the ICB are required to publish registers on their website detailing information on Gifts, Hospitality and Sponsorship received by ICB staff. These registers will detail offers made to staff and the ICB's response.

- *Register of Procurement Decisions*

To ensure the ICB is open and transparent in their spending of public money, information is required to be published on the ICB's website detailing procurement processes and decisions. This includes a register detailing who was involved in procurement decisions.

- *Freedom of Information Requests*

In certain circumstances, staff names, job titles work e-mail addresses and work phone numbers for staff at band 7 or above may be released to requesters under the Freedom of Information Act 2000. In accordance with the Act, this information is then placed on the ICB's Disclosure Log on its website.

- *Annual Report*

Certain senior members of staff, the Governing Body, will have their name, role, salary and pensions entitlements published annually as part of the ICB's Annual Report.

How we look after your information

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

At Board level, we have a Senior Information Risk Owner (SIRO), the Executive Director of Corporate , who is accountable for the management of all information assets and any associated risks and incidents, and a Caldicott Guardian, the Chief Nurse, who is responsible for ensuring the correct management of patient and staff information and confidentiality. Additionally, we have the Associate Director for Information Governance who is the ICB Data Protection Officer (DPO) who is responsible for the day to day management of Information Governance and ensuring that the ICB complies with its obligations under the DPA.

The DPO's main tasks include:

- Providing advice to the organisation and its employees on UK GDPR/DPA 2018 compliance obligations.
- Advising on when Data Protection Impact Assessments are required and monitoring their performance.
- Monitoring compliance with the UK GDPR/ DPA 2018 and organisational policies, including staff awareness and provisions for training.
- Co-operating with, and being the first point of contact for, the Information Commissioner's Office.
- Being the first point of contact within the organisation(s) for all data protection matters.
- Being available to be contacted directly by individuals.
- To take into account information risk when performing the above.

The ICB's DPO is, Dan Clement, Associate Director for Information Governance, and he can be contacted at kmicb.dpo@nhs.net

The ICB are committed to ensuring that personal and special category data is kept confidential and secure and used appropriately, and everyone working for the NHS has a contractual and legal duty to protect your information.

The confidentiality and security of personal and special category data is of paramount importance to the ICB, and we strive to ensure that all such information under our control is handled in accordance with all legal, professional and ethical obligations.

All staff have a responsibility to ensure that the policies and procedures are adhered to. Staff members are provided with mandatory annual Data Security Awareness training to enable them to fulfil their obligations:

- Access to identifiable information is strictly controlled and limited to only those with a legitimate need to access it (i.e. to enable them to fulfil their job role).
- Personal and special categories data is held in accordance with the requirements of the DPA 2018. We will not hold information any longer than is necessary, and when the relevant retention period has been reached, we will review the records and either retains the data for longer if required or dispose of it in a secure way.
- Anyone who receives personal or special category data from us is also under a legal duty to keep it confidential and secure as per the requirements of the DPA 2018. In instances where the ICB hold contracts for services, we ensure the data sharing agreements and monitoring in place provide sufficient assurance regarding the protection of your personal and special categories data.
- This Privacy Notice does not provide exhaustive detail of all aspects of our collection and use of personal confidential data. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the ICB's Head of Corporate Governance/Data Protection Officer using the contact details above.

Your rights regarding the information we hold about you
The DPA 2018 provides staff with rights regarding their own personal data, including the right to find out what personal data is held on computer and in paper records, and to view or be provided with a copy of this data within one month of receipt of such a request, this is called a Data Subject Access Request. In addition to the right of access, the DPA 2018 provides staff with the following rights:

- The right to be informed
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling
- The right to complain, judicial remedies and compensations

For further information regarding your rights, please see Appendix 1.

What if the data we hold about you is incorrect?
It is important that the information which we hold about you is up to date. If your personal details change or if they are currently inaccurate then it is important that you either update your details in ESR, or let us know by contacting your manager, and then complete a 'Change Form' via Topdesk.

Changes to our privacy notice: We keep our Privacy Notice under regular review and will inform staff of any changes.

Further information: For further information regarding your rights and how to exercise them, please see the ICB general Privacy Notice and the Guide to Data Subject Rights available on the staff zone. You can also contact the Data Protection Officer using the details above.

Purpose or activity	Data Controller	Data Protection Officer	Purpose of the processing	Lawful basis for processing *(Legitimate interests is no longer available to public authorities as a basis for processing in the performance of their tasks)*	Categories of personal data	Source of data (is this publicly accessible?)	Processor of personal data (The person or organisation which processes personal data on behalf of the ICB).	Details of transfer to third country and safeguards	Retention period	Existence of data subjects rights *For further information on how to exercise your rights please see the Your Rights (including opt outs and accessing your data)in the fair Processing Notice*							Is the provision of data part of a statutory or contractual requirement or obligation. Are there any consequences of failing to provide the personal data.	Details of any automated decision making
										Right to be informed	The right of access	The right to rectification	The right to erasure	The right to restrict processing	The right to data portability	The right to object		
Financial transaction	The ICB	Associate Director of Information Governance	Financial transactions such as payroll management, absence returns, travel claims, budget setting and monitoring, and financial audits include personal and/or sensitive data.	Article 6 (e) Public task Article (9) (2) provision of health or social care or treatment or the management of health or social care services.	Personal data and special category data including name, address, DOB, NHS number and healthcare information	Within the ICB.	Shared Business Services and payroll services (provided by Mersey and West Lancashire NHS Trust (MWL) , UNISON, Computershare, <u>Expenses are processed using Giltbyte</u>	None	6 years after the staff member leaves or 75th Birthday, whichever is sooner.	✓	✓	✓	X	✓	X	✓	The provision of data is a contractual obligation and can be a statutory requirement e.g. fraud reporting.	None
HR Processes	The ICB	Associate Director of Information Governance	HR processes will include personal and/or special category data, such as: • Staff change forms • Recruitment and selection • Sickness reporting • Payroll Administration • Electronic Staff Records • Occupational Health and Counselling Services • Childcare Voucher Scheme • Staff survey • DBS checks • HR audits • Workforce diversity data • Employee relations	Article 6 (b) Contract Article 9 (h) Employment and Social Security Staff survey Article 6(e) and Article 9 (h)	Personal data and special category data including name, address, DOB, NHS number and healthcare information	From employees. From Occupational Health (provided by East Kent Hospitals University NHS Foundation Trust)	Employees, ICB staff. Transactional HR services are outsourced to Kent Community Health Foundation Trust (KCHFT) utilising Topdesk, Trac and TAPs systems. Occupational Health (provided by East Kent Hospitals University NHS Foundation Trust) Payroll services (provided by Mersey and West Lancashire NHS Trust (MWL)) All HR information is held centrally on the ESR system which is hosted by IBM. In addition; DBS checks are carried out by Atlantic data ltd. -Childcare Voucher scheme. <u>- Bike Scheme</u>	None	6 years after the staff member leaves or 75th Birthday, whichever is sooner.	✓	✓	✓	✓	✓	✓	X	The provision of data is a contractual obligation and can be a statutory requirement e.g. fraud reporting.	None
Legal / Statutory obligations	The ICB	Associate Director of Information Governance	The ICB must comply with certain statutory and legislative requirements to share information with other agencies. Examples include: • ONS surveys • National Fraud Initiative • Department of work and pensions • HMRC • Central government departments • Law enforcement agencies The above list is not exhaustive.	Article 6 (c) Legal Obligation Article 9 (b) Employment and Social Security	Personal data and special categories data including any of the following name, address, DOB, contact details, salary information, pension information, job details.	From employees.	ICB processes data and shares with the following upon request: • Office National Statistics • Cabinet Office • Department of work and pensions • HMRC • Central government departments	None	6 years after the staff member leaves or 75th Birthday, whichever is sooner.	✓	✓	✓	X	✓	X	X	The provision of data is a contractual obligation and can be a statutory requirement e.g. fraud reporting.	None