DATA PROTECTION FOR STAFF

Policy and Procedure
DATA PROTECTION FOR STAFF
Responsible Persons:
Board Lead: Data Protection Lead

Circumstances may arise or there may be a change in guidance (e.g. NICE or Employment Law) where changes may be required to the policy before the planned review date. Staff are responsible for identifying this to the Manager who will then put in place a policy review process.
NOTE: All policies remain extant until notification of an amended policy is communicated to all staff by the responsible manager.

CONTENTS:

1. About this Policy

Every individual has rights in relation to the way in which their personal data is handled. This policy is intended to outline some information about those rights and how we intend to protect them. This policy is issued on behalf of City Health Federation.

As an employer, we collect, store and process personal data about our Staff. For the purposes of this policy the word "Staff" includes employees, workers, temporary or agency workers, consultants and contractors.

We recognise that it is important for us to respect the personal data that we collect and we are committed to collecting, storing and processing it in a lawful and confidential manner.

We will bring this policy to the attention of our Staff, and we will ensure that any members of Staff or third parties who have access to personal data and who are responsible for collecting, storing and processing personal data shall receive training on the correct lawful and confidential treatment of that data.

Any questions about the operation of this policy, or any concerns that this policy has not been followed, should be referred in the first instance to the Data Protection Lead.

This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. Some Helpful Definitions

Data Subject means any living individual about whom personal data is held. For the purposes of this policy, the Data Subjects are our Staff.

Data Controller means a person who, or organisation which decides what personal data will be collected, how and why. For the purposes of this policy, we City Health Federation are the Data Controller.

Data Protection Lead means the person responsible for overseeing this policy and the collecting, storing and processing of personal data by us. The person with responsibility for this role may change from time to time, but at the present time it is the City Health Federation Board Strategy Director.

Data User means any of our Staff whose work involves collecting, storing or processing personal data. This will vary depending on the personal data being collected, stored or processed. A large proportion of personal data will be restricted to members of management, HR and payroll, but it may be necessary for other members of Staff to be data users.

Data Processor means any person who, or organisation which collects, stores or processes personal data on our behalf. The number and identity of the data processors we use may change from time to time, but at the present time they include:

- Sage, the system used to process our payroll, containing personal data needed to calculate and pay any wages and benefits. This will include: name, address, date of birth, tax code and National Insurance Number, bank details, wages and benefits information, pension contributions, attachments of earnings or deductions from wages information, holiday dates,

sickness dates (but no other health information) and other absence dates, maternity paternity or adoption related dates and payments, etc.

- NHS Pensions, who operate our pension scheme and have access to personal data needed to carry out that service. This will include: name, address, date of birth, tax code and National Insurance Number, wages information, pension payments contributions and details of any beneficiaries of the scheme.

Processing means any activity that involves use of data electronically and manually. It includes collecting, recording, organising or storing the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Personal Data is data relating to a living individual who can be identified from that data – or from a combination of that data and other information in our possession. It may be factual (for example name, address or date of birth) or it may be an opinion about that individual, their actions or behaviour.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

3. What Personal Data will we collect?

To help you understand what we mean by personal data, here is a list of the types of personal data that we will collect, store or process in relation to our staff:

- Name and contact information including postal address, email address and phone numbers;
- National Insurance number and tax code;
- Application forms and CVs.
- Offer letter, references obtained and given, and criminal record checks;
- Wages and benefits information, contract of employment and any variations to your contract of employment or other terms and conditions relating to employment;
- Bank details;
- Correspondence, minutes, forms and other documents relating to qualification, training, appraisal and performance management;
- Correspondence, minutes, forms and other documents relating to grievance procedures, or complaints of discrimination, bullying and harassment, or whistleblowing;
- Correspondence, minutes, forms and other documents relating to disciplinary investigations and procedures;
- Correspondence, minutes, forms and other documents relating to absence management procedures;
- Data relating to an individual's medical history including any medication taken (if notified to us), any medical conditions (if notified to us), absence dates and reasons given for absence, return to work documents, doctors' fit notes or other correspondence from medical advisors,

medical records and reports (these will not be obtained without the individual's consent) accident reports, alcohol or drug testing records;

- Family member information/ next of kin information.

Over time, we may need to collect other forms of personal data and, if we identify any, we will let you know.

In most cases, we will collect personal data from you directly. However, there may be some types of information that we need to collect from a third party. This may include: tax information from HMRC, attachments to earnings information from the Court Service, a reference from your former employer(s), your unspent criminal convictions from the Disclosure and Barring Service, notification of absences and reasons for absence from a family member or friend if you're not able to make the notification yourself, and fit notes and correspondence from your GP or other healthcare professionals.

4. What Sensitive Personal Data will we collect?

We will try to limit the sensitive personal data that we collect. It is our intention to collect sensitive personal data only about:

- Your health – sensitive personal data may be recorded if you notify us of any medication you are taking or any health conditions you have, or it may be recorded in records of absence and absence notification, return to work documents, and doctors' fit notes or other correspondence from medical advisors. If we believe it is necessary to obtain access to your medical records and or to request a medical report from your GP or healthcare professional or from an independent healthcare professional such as the government's Fit For Work service or an occupational health advisor, we will ask you to give your consent to this before we do anything and we will remind you that you do not have to give your consent if you do not want to.
- Your trade union membership – this may be recorded if you are invited to a meeting, such as a disciplinary hearing, at which you are entitled to have a trade union representative present.

It is not our intention to collect sensitive personal data about your racial or ethnic origin, political opinions, religious or philosophical beliefs, sex life or sexual orientation. However, it is possible that we may become aware of this sensitive personal data as we get to know you. If you choose to disclose information about your ethnic origin, political opinions or religion etc. we will treat this confidentially.

If we ask you to complete an equal opportunities monitoring questionnaire this will be done on an anonymous basis and the data collected will be held anonymously and separately to any other data that we have about you.

5. Why do we collect, store and process personal data?

We will only collect, store and process personal data to the extent that it is required for the purposes set out below (and in any separate privacy notice issued to you).

We need to collect, store and process personal data in order to fulfil the terms of our contract with you and to meet our legal obligations as an employer, and in order to ensure that we comply with

good HR practices for managing Staff and meet the needs of our business. This personal data will be accessible only by the Business Administration team, the Directors and senior management, and your line manager. For example:

- We need contact information like your full name, address, telephone number(s) and email address so that we can keep in touch with you, but we will not pass your contact details on or use them for marketing to you without your consent.
- We need to check your passport and/or visa or residence permit and similar information to ensure and be able to evidence that you have the right to work in the UK.
- We need to check your criminal record, but will limit this check to unspent convictions. We need to do this because you will be working in a position of trust.
- We need information like your bank details, tax code, National Insurance number, student loan information, any attachments of earnings orders and your date of birth for administration of salary, benefits, and pension contributions.
- We will create a personnel file for you, which will include the above information, your CV and/or application form, your offer letter, any references obtained in relation to you, your contract of employment and any amendments to it, information provided to us by you in relation to your health, and personal data that we create and collect during your employment such as information relating to performance reviews and appraisals, training, promotions and job changes, accident records, sickness absences (including self-certification forms and return to work forms, fit notes, doctors' reports and notes of any review meetings or capability meetings), maternity, paternity, adoption or parental leave, other time off work, disciplinary matters, grievances, whistleblowing procedures, redundancy programmes (including selection criteria and scores) and transfers of employment**.**

We have Closed Circuit Television (CCTV) cameras in some of our premises and these will record your image if you are within range of them. However, in order to ensure your privacy, the CCTV cameras will not record sound and so your conversations will not be recorded. In these premises, CCTV footage may be viewed by the Security team, the HR department, the Directors and senior management, and your line manager. CCTV footage will be used for the purposes of: securing our premises and ensuring the safety of our Staff, appraisals and performance management of Staff (including training, performance reviews and disciplinary processes), dealing with grievances and complaints raised by Staff and by members of the public, dealing with any claims brought against the business or our Staff by Staff and members of the public, ensuring that our policies and procedures are complied with, investigating alleged breaches of our policies and procedures, and assisting the appropriate authorities in investigating and/or prosecuting any actual or potential criminal act against the business or our Staff.

We will monitor the use of our telephones, internet and email systems and social media websites. This monitoring may include: logs of incoming and outgoing telephone calls including numbers used, times of calls and duration of calls; incoming and outgoing emails including email addresses, times of emails, size of emails, subject headings and attachments, we may also read the content of emails; websites visited, when and for how long; and, content of social media pages. This monitoring will be carried out by the IT company and will be accessible only by the IT department, the HR department, the Directors and senior management, and your line manager. The purposes of this monitoring is

limited to ensuring that our policies and procedures are complied with, investigating alleged breaches of our policies and procedures, investigating alleged breaches of confidentiality or disclosures of intellectual property information or trade secrets, investigating any derogatory comments or misrepresentations made in relation to our business or our Staff, investigating grievances or disciplinary matters, covering a member of Staff's work if they are absent from work for any reason, finding any lost messages or information, and complying with any legal obligation.

6. Who do we share your Personal Data with?

We will share your personal data with the Data Processors identified above.

If you have an accident at work or are taken ill, it may be necessary for us to call an ambulance for you and to disclose personal data (including sensitive personal data) about your health and/or medication to the medical professionals in attendance. If you are unconscious or very unwell, it may not be possible for us to ask for your consent in relation to this disclosure and we will limit the disclosure to the information required to be disclosed in your best interests.

If we lose a contract that you are engaged to work on or if a part of our business that you are engaged to work in is bought by another organisation, then it is possible that your employment will transfer to the other organisation. We will consult with you about the transfer of your employment if that arises. However, as part of this process, we might have to transfer some personal data about you to the other organisation so that they can get ready to employ you – this may include your name, job title, salary and benefits information, terms of employment and any disciplinary or grievance procedures followed in the two years before the transfer.

We may also have to disclose personal data in order to comply with our legal obligations, to enforce or apply any contractual terms that we have with you, or to protect our rights, property, or safety of our Staff, customers or others. This may include instructing legal advisors and engaging in legal proceedings, and exchanging information with other organisations for the purposes of fraud protection and credit risk reduction.

We will not send your personal data outside of the UK.

7. How long do we keep Personal Data?

We will ensure that any Personal Data that we hold is accurate and kept up to date. We will check the accuracy of Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

We will not keep Personal Data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

As explained above, we will create a personnel file for you and we will keep this for the duration of your employment and for a minimum of six months after you leave your employment. After six months, we will review your personnel file and delete any personal data that we do not need. We will retain the following personal data for the following periods of time:

Data	Period of Time
Data confirming payments due to you. For example, your contract of employment and any information about salary or benefits.	6 years after you leave your employment.
Data confirming payments made to you.	6 years after you leave your employment.
Data relating to taxes, National Insurance contributions and other charges paid in relation to you.	7 years after you leave your employment.
Data relating to any accidents or injuries at work.	3 years after you leave your employment.
Data relating to any references given in relation to you.	1 year after the date of the reference.

Any personal data collected via our GPS trackers and CCTV footage will be stored in accordance with the terms of the GPS tracker/ CCTV monitoring service or for a period of up to three months after the date on which the CCTV footage was recorded and will then be deleted or recorded over unless in exceptional circumstances which require the CCTV footage to be stored for a longer period, such as actual or potential criminal proceedings against a member of Staff or a member of the public.

8. How will we keep your Personal Data secure?

We will put in place appropriate procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction and to prevent unlawful or unauthorised processing of personal data, and accidental loss of or damage to personal data.

Only people who are authorised to access or use personal data will have access to it.

Personal data held in paper records will be stored in locked filing cabinets and cupboards, locked desk drawers and/or locked offices. We will secure our premises by ensuring they are locked when not in use and areas where personal data are stored are secured with security card/key pad entry doors. Staff must ensure that these locks and cards are used and premises kept secure. Any strangers seen on the premises should be reported to main reception.

Personal data held in electronic records will be stored on secure servers that are regularly backed up and subject to regular maintenance. Passwords and restricted networks will be used to limit access to electronic records. Staff must ensure that they lock their IT equipment using appropriate passwords and that extra care is taken when transporting IT equipment, particularly on public transport.

Personal data will only be transferred to Data Processors who put appropriate security measures in place.

Personal data will be securely destroyed. Personal data held in paper records will be shredded or placed in confidential waste. Personal data held in electronic records will be deleted. Digital storage devices will be wiped and/or destroyed when they are no longer required.

9. What are your rights in relation to your Personal Data?

You have certain rights in relation to your personal data. The first of these is to be provided with a "privacy notice" which sets out information about what personal data will be collected and why. This policy is a privacy notice.

You also have a right to have access to your personal data to confirm what personal data we are holding and to check that it is accurate and up to date. If the personal data that we hold is not accurate or up to date, you have the right to correct it. If you would like to access your personal data, you should make a request in writing to the Operational Support Manager– this is called a Subject Access Request. They will respond to your request within 30 days. Please note that if a document contains your personal data and another person's personal data then they may need to cover up the other person's data to protect their privacy.

You have the right to object to us collecting, storing and processing your personal data and to ask us to delete it. If you wish to object, you should bring this to the attention of the Operational Support Manager in writing. They will arrange a meeting with you to discuss which category of personal data it is that you don't want us to collect, store or process. They will explain the reasons why we collect, store or process that data and, if you are still concerned, they will talk to you about your reasons for objecting and agree a way forwards with you. If the personal data in question has been collected, stored or processed in order to enable us to fulfil the terms of our contract with you and to meet our legal obligations then it is unlikely that the Operational Support Manager will be able to delete the personal data. If the personal data in question has been collected, stored or processed in order to meet a genuine business need, the Operational Support Manager will have to balance that need against your concerns and decide whether to delete the personal data. If the personal data in question has been collected, stored or processed for any other reason, then the Operational Support Manager should be able to delete the personal data. The Operational Support Manager will let you know their decision and the reasons for it. If the personal data has been collected, stored or processed unlawfully or outside of the scope of this policy, or where the storing and processing of the data is no longer necessary for the purposes that we have stated in this policy, then the Operational Support Manager should be able to delete the personal data.

10. What are your obligations?

You need to take care of your own personal data. For example, if you are going to submit a sick note to us then make sure that this is in an envelope and marked confidential for the attention of the Operational Support Manager. As a further example, if you are given a copy of your contract of employment, or a letter about your salary or a disciplinary procedure, you should make sure that you keep this safely in your bag before taking it home.

You also need to consider that you may choose to disclose personal data on social media pages such as Facebook, which are not private forums and may be viewed by any members of management or colleagues that you 'friend' or 'follow' and may also be viewed by people you do not 'friend' or 'follow' depending on your privacy settings.

You need to take care of other people's personal data. If you are given a member of Staff's personal data then you must respect that data and act in accordance with the terms of this policy. For example, if you are given a colleague's sick note to hand in to management or if you come across a

letter or payslip that someone has dropped, you should hand that in to the Operational Support Manager for safekeeping without reading or disclosing the information in it.

If you are in a role which involves data protection duties, such as line management or HR management, you must make sure that you keep personal data in accordance with the terms of this policy and any training that you have been given. In particular:

- You must only collect, store and process the categories of personal data identified in this policy and for the purposes set out in this policy.
- If you need to collect, store and process different categories of personal data or for another purpose, you must inform the Operational Support Manager and they will decide whether a separate privacy notice should be issued to Staff and whether consent is needed from the Staff before proceeding.
- You must ensure that the personal data you are responsible for is kept up to date and allow Staff to access and update or correct their personal data if they request this.
- You must ensure that personal data is stored securely, for example in a locked filing cabinet or in a password protected email account or word file. You will receive training on the security measures we expect you to take.
- You must not transfer personal data to any third party, other than those specified in this policy or a separate privacy notice (as approved by the Operational Support Manager) and you must not transfer personal data outside of the UK.
- You must ensure that personal data is not kept for longer than the time periods stated in this policy.
- If you receive a Subject Access Request from a member of Staff, you should contact the Operational Support Manager who will be able to assist you in responding to it. If the response is received by telephone or in writing, you should take reasonable steps to confirm the identity of the person making the request and should only send personal data to the address that we hold for them.

11. Consent

Please note that, the personal data we have outlined is collected, stored and processed for the specific reasons listed and in order to fulfil the terms of our contract with you, to meet our legal obligations as an employer, and meet the needs of our business. As such we do not need you to give your express consent to the collection, storage or processing of this personal data.

There may be instances in which we wish to collect, store or process additional personal data or sensitive personal data for which we will need you to give your express consent. For example, if we would like to obtain access to your medical records or a report from your doctor, or if we would like you to take part in a consultation with the Government's Fit For Work service or an occupational health advisor. In these circumstances, we will explain to you in writing what personal data we need and why, whether we need to disclose your personal data to any third party - who and why, how long we will store the personal data, your rights of access to the personal data, your options for consenting or refusing to consent or withdrawing consent, and the implications of consenting or refusing to consent or withdrawing consent.

We reserve the right to change this policy at any time. Where appropriate, we will notify Staff of those changes in writing.