DATA PROTECTION POLICY AND PROCEDURE

This Policy was approved & authorised by:

Name: Kate Jensen

Position: Centre Manager

Date: November 2023

Signature: K Jensen

Policy review date: November 2024

Contents

Introduction

The aim of this policy is to comply with relevant legislation in regard to the keeping of employment records and customer data. Wigton Youth Station (Wigton Youth Station) requires personal information relating to each individual in order to manage its business in an efficient and effective manner. As such, it is essential that Wigton Youth Station ensures that arrangements for collecting, processing, storage and disposal of personal data complies with the Data Protection Act 2018/ General Data Protection Regulation (GDPR).

Definitions

The GDPR applies to 'controllers' and 'processors'

- A '**Data Controller**' means a person who (either alone or jointly) determines the purposes for which and the manner in which any person data are, or are to be, processed. This would be Wigton Youth Station all staff are responsible to ensure all data within our organisation is processed within the terms of this policy.
- A '**Data Processor**' is responsible for processing personal data on behalf of a controller. This would be any work carried out by Wigton Youth Station on behalf of a organisation e.g. Youth Work Tenders.
- **Information Commissioners Office (ICO)** this is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
- **Personal data** is information that relates to an identified or identifiable individual. What is personal data? Anything which can identify a living human being, It includes: Name; Address; Phone Number; Picture; Voice; National Insurance Number; IP Address. It includes computerised data, manual data and any other form of accessible record that includes personal information held by the Wigton Youth Station.
- A **data subject** is an individual that is the subject of any personal data.

POLICY

It is the intention of Wigton Youth Station to adhere to the principles of the GDPR (the Act). Therefore, the data protection policy applies to all employees (there is also a separate GDPR statement for all employees- appendix A of this policy). Further to this it also imposes obligations on those who process data for or on behalf of Wigton Youth Station. Wigton Youth Station is committed to a policy of protecting the rights and privacy of individuals in accordance with the GDPR.

The GDPR is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with employees & service users about the use of information about them and by following good data handling procedures. The regulation is mandatory and all organisations that hold or process personal data must comply.

The regulation contains 7 principles.

- Personal data should be processed fairly, lawfully and in a transparent manner.
- Data should be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.
- The data should be adequate, relevant and not excessive.
- The data should be accurate and where necessary kept up to date.
- Data should not be kept for longer than necessary.
- Data should be kept secure.
- Organisations are accountable for the data they hold and must demonstrate compliance with the principles

Wigton Youth Station will inform any data subjects:

- What information Wigton Youth Station holds about them.
- How to gain access to the data.
- How to keep data held up-to-date.

Policy Statement

Organisation's must have a valid reason for having personal data and the data should not be held for any longer than necessary. Therefore, Wigton Youth Station will only hold personal data of service users who attend our project.

The Act lays down regulations and safeguards for the collection, recording and use of personal information whether on paper, in a computer or recorded on other material. Wigton Youth Station needs to collect, hold and use certain types of information about people whom it deals with in order to operate. This is primarily young people but also employees, volunteers, board members, and other adults whom are connected with Wigton Youth Station through a variety of different means. Certain information may be required for regulatory or monitoring purposes as laid down by statue. Other information may be required from time to time for other means. In any case the Wigton Youth Station recognises that the information must be dealt with lawfully and correctly under the principles laid down within the Act.

Employees must not use any information obtained in the course of their employment for personal gain or benefit, nor should they knowingly pass it on to others who might use it in such a way. Employees must not communicate confidential information or documents to others who do not have a legitimate right to know. Furthermore, such information which is stored on computer systems must only be disclosed in accordance with the requirements of the GDPR.

GDPR act. Those employees responsible for holding confidential data will be provided with appropriate training and advice do this by their line manager. We will however always do the following:

- Consent will be sought to keep personal details on file
- It will be kept secure
- Information will be confidential

Implementation of the Policy

Overall responsibility for policy implementation and review rests with The Board of Trustees for Wigton Youth Station. However, all employees are required to adhere to and support the implementation of the policy. Wigton Youth Station will inform all existing employees about this policy and their role in the implementation of the policy. They will also give all new employees notice of the policy on induction.

Policy Amendments

Should any amendments, revisions, or updates be made to this policy it is the responsibility of Wigton Youth Station's senior management to see that all relevant employees receive notice. Written notice and/or training will be considered.

Additional Information

If you require any additional information or clarification regarding this policy, please contact your manager. In the unlikely event where you are unhappy with any decision made, you should use Wigton Youth Station's formal Grievance Procedure.

To the extent that the requirements of this policy reflect statutory provisions, they will alter automatically when and if those requirements are changed.

PROCEDURE

Accountability and governance

We must be able to demonstrate compliance with the GDPR:

- The establishment of a governance structure with roles and responsibilities.
- Keeping a detailed record of all data processing operations.
- The documentation of data protection policies and procedures.
- Data protection impact assessments (DPIAs) for high-risk processing operations.
- Implementing appropriate measures to secure personal data.
- Staff training and awareness.
- Where necessary, appoint a data protection officer.

Personal Data

The GDPR applies to any organisation that handles personal data. An individual who holds data about another individual on a personal level, for example a family members telephone number stored in a phone, will not need to consider GDPR for that particular data.

Personal data is data that relates to an identified or identifiable individual and is:

- processed electronically
- kept in a filing system
- part of an accessible record, for example an education record
- held by a public authority.

This includes data that does not name an individual but could potentially identify them. For example a payroll or staff number. Employers should ensure staff are aware that any personal data they have in their possession will also be subject to the regulation. For example, if a manager has a written copy of contact details for their team or an employee keeps service user names and numbers on post it notes on their desk.

An organisation must have a lawful basis for handling any personal data.

How long can information be kept?

Information must not be kept for longer than is necessary.

While there is no set period of time set out within the GDPR, some records must be kept for a certain period of time in accordance with other legislation. For example, HMRC require payroll records to be kept for three years from the end of the tax year that they related to. Funders also have stipulations on how long we keep certain records. This differs from funder to funder.

How long will Wigton Youth Station keep young people's personal data for?

We will keep young people's personal data for 5 years from when they have left Wigton Youth Station, unless we feel this data is sensitive then we will keep this data for 8 years. Examples of sensitive data are safeguarding referrals made to the Safeguarding Hub and those involved in the early help processes.

Your Responsibilities as a Data Handler

Digital technology has transformed almost every aspect of our lives in the twenty years since the last Data Protection Act was passed. All staff have a responsibility to ensure that their activities comply with the data protection principles.

Therefore, we are legally responsible for protecting data held on computers as well as Wigton Youth Station. Employees could face prosecution and fines for knowingly or recklessly disregarding the requirements of the Act.

What you must do (as a Controller)

The following guidance is not exhaustive. It is intended as an indication of good practice. Please refer to your line manager for specific instructions.

- Only obtain personal data from those necessary
- Satisfy yourself that the data you obtain is accurate
- Keep input secure, e.g. keep VDU's out of public view and screens clear when not in use. Laptops, computers, mobile phones, external hard-drives & USBs must have a password. The Wigton Youth Station manager must have passwords to these devices.
- Keep output secure e.g. external hard-drives, USB storage sticks & printouts should not be left out when not in use; protect passwords; dispose of data appropriately. Do not give information over the phone, but ask the caller to write in; take care not to disclose data unintentionally through casual conversation.
- At the end of each shift staff should ensure that all data is securely locked away.

Management Responsibilities

Managers have responsibility for the type of personal data they collect and how they use it. Staff should not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

If employers are monitoring their staff, for example to detect crime, they are required to make their workers aware of the nature and reason for the monitoring. This is applicable whether the monitoring is taking place using CCTV, accessing a worker's email or telephone calls or in any other way.

Employers (Controllers) Responsibilities

To ensure its compliance to the GDPR, an organisation must:

- have a clear retention policy for handling personal data and ensure it is not held for longer than is necessary
- have a legal basis for acquiring and/or using any personal data
- ensure that all staff are aware of the retention policy and follow it
- respond to subject access requests (sometimes called personal data requests) within one month
- **if there is a personal data breach that is likely to result in a risk to the rights and freedom of an individual, inform the ICO within 72 hours and, if the risk is deemed to be high, also inform the individual concerned.**

Parental consent

As we have always done, we will seek the parental consent of our children and young people to hold and share data. The GDPR sets a high standard for consent.

Consent means offering people genuine choice and control over how you use their data. You can build trust and enhance your reputation by using consent properly.

The GDPR builds on the 1998 Act standard of consent in several areas and contains much more detail:

- You should keep your consent requests prominent and separate from other terms and conditions.
- Seek a positive opt-in such as unticked opt-in boxes or similar active opt-in methods.
- Avoid making consent a precondition of service.
- Be specific and granular. Allow individuals to consent separately to different purposes and types of processing wherever appropriate.
- Name your business and any specific third-party organisations who will rely on this consent.
- Keep records of what an individual has consented to, including what you told them, and when and how they consented.
- Tell individuals they can withdraw consent at any time and how to do this.

A worker's right to request their personal data

Workers have a right to access information that an employer may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes.

If a worker wants to see their personal data, they should speak to their employer. Most requests for personal data can be provided quickly and easily.

If the employer is unable or unwilling to agree to the request, a worker could make a Subject Access Request. A subject access request should be in writing and include:

- full name, address and contact details
- any information used by the organisation to identify the worker (account numbers, unique ID's etc.)
- details of the specific information required and any relevant dates.

The time limit to deal with Subject Access Requests is one month under the GDPR.

While the Data Protection Regulation allowed an employer to charge a fee for Subject Access Requests, fees may only be required under GDPR if the requests are "manifestly unfounded or excessive".

If an employer refuses a request they must inform the individual within one month:

- why they have refused the request
- that the individual has the right to complain to the supervisory authority and to a judicial remedy.

Disclosure of Information

Staff need to be very careful when disclosing information especially over the phone, *eg- A parent rings to ask if their child had attended youth club last week? Staff should consider responding to the registered email on the consent form, instead of having a conversation over the phone.*

How?

We can 'disclose' information (i.e. give it to others) by a range of different means – VDU display, printed or handwritten documents, microfilm, or by word of mouth. All of these methods are covered by the Act.

What?

All personal data held in computerised from is covered by the Act, no matter how unimportant or trivial it may seem to you.

Who to?

Personal data may only be passed to those persons who we work in partnership with such as police, Childrens Services, schools. You should check who can receive such information with your manager.

APPENDIX A

General Data Protection Policy-Staff

Wigton Youth Station is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all employees, workers and contractors.

Wigton Youth Station is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained within this document.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving licence.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- Photographs.
- We may also collect, store and use the following "special categories" of more sensitive personal information:
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies (where applicable) or other background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest [or for official purposes].

Situations in which we will use your personal information

We need all the categories of information as listed primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing company benefits (where applicable).
- Liaising with your pension provider.
- Administering the contract, we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. Where we need to carry out our legal obligations or exercise rights in connection with employment.

2. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations (where applicable).

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about members or former members in the course of legitimate business activities.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We do not transfer your personal information outside the EU.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and (where applicable) other entities within our group.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our charity as part of our regular reporting activities on the charity's performance, in the context of a restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the charity. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. In order to determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.
- If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact Kate Jensen in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. In order to withdraw your consent, please contact your Manager in writing (including the legal basis for your belief that your consent can be withdrawn). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact your Manager.

Signed ..... Date .....

Print Name .....