Privacy and Data Protection Policy

1. Introduction

Working Links is committed to protecting the rights and privacy of individuals in accordance with the EU General Data Protection Regulation (GDPR). The Business needs to process (store or use) certain personal data about its employees, agents, contractors, advisers, service users and customers in order to fulfil its purpose and to meet its legal obligations.

We process personal information for the performance of a contract to enable us to provide advice and professional services as an employment agency and trainer and support statutory requirements in the rehabilitation and offender management services across our three Community Rehabilitation Companies (CRC) in Wales; Bristol, Gloucestershire, Somerset and Wiltshire (BGSW); and Dorset, Devon and Cornwall (DDC).

2. Scope

This Policy applies to all employees (including Contractors, Secondees, Agency personnel, Contracted Third Parties) who have access to Information Systems (applications, infrastructure, third party managed systems and so on.). All access to customer and employee personal data, whether it is stored electronically or in paper-based records, shall comply with the Data Protection Policy.

This policy is applicable regardless of location, e.g. working from an office, home or elsewhere.

3. Personal data and how we handle it

In order to provide our services, we need to collect and process personal data about you and may disclose this information to third party service providers. This includes collection of any sensitive data as defined within the General Data Protection Regulation, such as medical history or criminal convictions, or additional data collected by us. You confirm your explicit consent to such data being processed by ourselves or any third party providers we may use. Before you provide us with any information about other people, you must first get their permission. This applies to all information you provide about them, but especially to sensitive data such as health information, or criminal proceedings or convictions. In submitting their details, you are confirming to us you have their permission to do so, and they understand how their information will be used under the terms of this Data Protection Policy.

All personal information you provide will be held in the strictest confidence and only used for the purpose of providing our service, subject to certain exemptions as described within this Data Protection Policy. From time to time there may be a requirement to process your personal data in other countries outside of the European Economic Area where data protection safeguards differ to those of the UK. Where this is necessary for the performance of a contract and your interests, we will ensure your data is kept securely and only processed in accordance with the GDPR. Some of our service providers may also process your data in other countries when agreed with Working Links, and we will request your data is kept securely at all times and the same UK security standards are met.

Authorised users will also disclose personal data and sensitive personal data to the HMPPS and DWP data controllers. Likewise an authorised user may have personal data and / or sensitive personal data disclosed to them by the Data Controllers. It is critical that disclosures to third parties

are provided with explicit consent from the customer or service user. In some circumstances areas will be required to make disclosures of information under the exemption clauses of the GDPR.

If the information (HMPPS and DWP) were to be subject to unauthorised third parties there is a risk that 'harm' may come to the data subject of the personal information and potentially expose the Working Links Group to litigation, therefore all users must comply with the Data Classification and Handling guidelines (in accordance with the Government Security Classification Policy and CESG requirements).

What is Personal data?

- Personal data is information (including opinions) which relates to an individual and from which he or she can be identified either directly or indirectly through other data which Working Links has or is likely to have in its possession. These individuals are sometimes referred to as data subjects.

What is Personal sensitive data?

- Sensitive data relates to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, criminal convictions or the alleged commission of an offence.
- Processing of Criminal Data will be under the control of systems compliant to the official authority and will only be shared with other organisations under the Data Protection exemption clauses: to prevent, investigate, detection or prosecution of criminal offences including public security.

4. Responsibilities

Working Links is the data controller or the data processor of the personal data we process and therefore are responsible for ensuring our systems, processes, suppliers and Working Links employees, agents, contractors and advisers comply with data protection laws in relation to the information we handle.

Others working for/on behalf of the business, usually third parties, who handle personal data in connection with the business, must operate in accordance with the GDPR and details of such processing should be the subject of written agreements between the business and the Third party.

Everyone who processes personal data in the business is responsible for ensuring adherence to the Data Protection Principles, in the case of third parties providing the personal data of others, the right to disclose this personal data.

Access rights to information shall be allocated to users, based on the minimum privileges required to fulfil the users' job function. Access privileges shall be authorised by the appropriate Information Owner.

We shall provide employees with induction training and ongoing training to support compliance with this Data Protection Policy and ensure all authorised users are sufficiently informed of their duties, obligations and liabilities in accordance with the data protection act and General Data Protection Regulation (GDPR).

We develop, maintain, and publish procedures and standards to achieve compliance with this Data Protection Policy in order to:

- Protect the data subject and the organisation from compromise of personal information
- Ensure that authorised users and Local System Controllers comply with the Data Protection principles

- Provide a secure Information Security Management System in compliance with ISO 27001:2013
- Comply with the Common Law Duty of Confidentiality

We have a Data Protection Officer who oversees compliance with data protection laws and this policy and provides guidance and advice to Working Links and Working Links employees, agents, contractors and advisers as required.

5. Principles of Data Protection

We have adopted the following principles to govern our use, collection and disclosure of personal data. These principles have been established to create a uniform standard across our offices worldwide taking account of the laws in the jurisdictions where we operate.

Working Links core principles provides personal data must:

5.1 Principle 1 - Obtain and process fairly and lawfully

- At the time when we collect information about individuals, we will make them aware of the uses for that information
- We will make people aware of any disclosures of their data to third parties
- We will obtain people's consent for any secondary uses of their personal data, which might not be obvious to them or for purposes that may arise in the future
- We will ensure that our data-collection practices are open, transparent and up-front

5.2 Principle 2 - Collected for specified, explicit and lawful purposes

- We will be clear about the purpose (or purposes) for which we keep personal information
- We will advise all individuals on our system about the purpose of our data collection practices
- We are registered with the Information Commissioner's Office, our register entry includes a comprehensive statement of our purpose
- We will maintain a list of all data sets and we will record the purpose associated with each

5.3 Principle 3 – Ensure that it is adequate, relevant and not excessive

- We shall retain only the minimum amount of personal data which is needed to achieve our purpose
- We will periodically review to make sure that all the information we collect is relevant, and not excessive, for our specified purpose

5.4 Principle 4 - Keep it accurate and up-to-date

- We shall ensure that any personal data is accurate and current and where discrepancies are found, the data will be amended or erased without delay.

5.5 Principle 5 - Retain it no longer than is necessary for the specified purpose or purposes

- We shall ensure that any personal information is not held for longer than required and, by applying checks to determine the length of time information is held, make sure that personal data is purged in an appropriate manner once the retention period has expired
- Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, not be considered to be incompatible with the initial purposes

5.6 Principle 6 - Keep it safe and secure

- Appropriate technical and organisational measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of the data and against accidental loss or destruction of, or damage to personal data

6. Collection, use and disclosure

As a company the type of data we collect and process falls into one of the following categories:

- personal data relating to subscribers to our newsletters and other promotional materials;
- personal data obtained and created in relation to providing our services; and
- personal data relating to our employees, agents, contractors and advisers.

6.1 Individuals' Rights

Personal data must be processed in line with individuals' rights, including the right to:

- request a copy of their personal data;
- request inaccurate personal data is corrected;
- request personal data is deleted and destroyed when causing damage or distress;
- right to Erasure (‘Right to be Forgotten’)
- right to data portability – transferred from one provider to another
- right to withdraw consent at any time
- rights in relation to automated decision making and profiling
- opt out of receiving electronic communications from us.

Should you wish to make a request in line with your rights as an individual, please forward it to the Data Protection Officer.

Working Links employees, agents, contractors and advisers must notify or inform the Data Protection Officer immediately if they receive a request in relation to personal data which Working Links processes.

6.2 Personal Data for Persons under 16 years of age

If you are under 18 year old you will need the consent of your parent or guardian to provide us with your personal data. Where we have reasonable belief no such consent is given, or we are told consent has not been given, we will delete any and all of your personal data and will not be able to collect this data until consent has been given.

7. Data retention

Under the GDPR there is a requirement to retain personal data for no longer than necessary to meet the purposes for which it was collected including all personal information processed to comply with the obligations in our contracts including retention periods.

Archived and current records will be disposed of securely aligned to retention periods and contractual disposal requirements (refer to our Data Retention Schedule).

8. Data Disposal

Our IT asset disposal provides sufficient guarantees about its security measures. Securely sanitise - destroy completely - disintegrate, pulverise, melt or shred. Laptop/PC hardware disks and USB memory pens must be sanitised / destroyed in line with HMG Information Assurance Standard No5.

9. How to make a complaint

You should direct all complaints relating to how we have processed your personal data to the Data Protection Officer.

Our employees, agents, contractors and advisers must inform the Data Protection Officer immediately if they receive a complaint relating to how we have processed personal data so our complaints procedure can be followed.

10. Security

Information security is a key element of data protection. We take appropriate measures to secure personal data and protect it from loss or unauthorised disclosure or damage. We have implemented appropriate security controls to ensure:

- The ongoing confidentiality, integrity and availability and resilience of processing systems and services.
- Where appropriate, use measures such as pseudonymisation and encryption.
- Measures to enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

11. Transfer of data between jurisdictions

We also use a number of suppliers in connection with the operation of our business and they may have access to the personal data we process. For example, an IT supplier may see personal data when providing software support. When contracting with suppliers and/or transferring personal data to a different jurisdiction, we take appropriate steps to ensure there is the same level of protection in place and the principles are adhered to.

12. Transfer to third parties

We must ensure that personal data is not disclosed to unauthorised third parties. All employees must exercise caution when asked to disclose personal data held on an individual to a third party.

We may disclose personal data to third parties where the data subject has given their consent and we and the partner have sharing arrangements in place.

Under some circumstances we will be required to make disclosures of information to third parties by law, e.g. police, or to the courts. Under these circumstances disclosure can be made without breaching the consent under specific circumstances:

- to protect the vital interests of a data subject
- to comply with the law; (e.g. where disclosure is required by or under any rule of law or by the order of a court, personal data are exempt from the non-disclosure, in these cases legal obligation overrides any objection the data subject may have)
- to assist in the prevention or detection of crime
- in connection with legal proceedings
- where the safety of a child is paramount

13. Non-conformance

All our employees, agents, contractors and advisors must abide by this policy when handling personal data and must take part in any required data protection training. Any breach will be investigated thoroughly and the individual may be subject to disciplinary action in accordance with Working Links Disciplinary Policy.

14. Definitions

The following terms have the following meanings:

“Client”	any person or organisation to whom we provide a service and who is identified as a client on our management system
“Contact”	an individual who is a contact of ours, including any client, any potential or former client, any supplier, any consultant, or any another professional advisor and any other contact of ours
“CRM”	our client relationship management system
“Data”	recorded information whether stored electronically, on a computer, or in certain paper-based filing systems
“Data Controller”	a person who or organisation which determines how personal data is processed and for what purposes
“Data Protection Officer”	the person designated as the Data Protection Officer from time to time
“Individual” or “You”	the person whose personal data is being collected, held or processed
“IS Policy”	our Information Security Policy
“Personal data”	please see the what is personal data section of this policy
“Employees, agents, contractors and advisors” or “PM person”	means partners, members, consultants, employees, temporary workers, agency and casual workers, contractors, collaborators, volunteers and those on work placements providing services to/working for Working Links
“Policy”	the Privacy Policy as amended from time to time
“Principles”	the core data protection principles set out in the Privacy Policy and summarised in our Data Protection Manual
“Process” or “Processing”	any activity involving use of personal data. It includes obtaining, recording or holding the personal 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

	as a result of those third parties having access to it.
“Medical Data”	Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, under the responsibility of a professional subject to the obligation of professional secrecy.
“Criminal Data”	Article 9 of GDPR states processing of personal data relating to criminal convictions and offences or related security measures based hall be carried out only under the control of official authority. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Document control

This policy will be reviewed at least annually to respond to any changes. Please refer to the policies page of the group intranet for the latest version.

Version	Date	Change details	Author / Editor / Reviewer	Approved by (if required)	Approval date (if required)	Next review date
1.0	17/05/2018	Policy published		GDPR Project Board		17/05/2019