Data Protection Policy

This Policy should be read in conjunction with the Privacy Notice on our website.

Thames Valley Partnership needs to gather, collect and use certain information about the individuals it comes into contact with in order to continue with its work. This includes employees, associates, suppliers, business contacts, supporters, volunteers, clients, board members and others.

This Policy along with the Privacy Notice aims to ensure that Thames Valley Partnership:-

- Complies with current legislation;
- Protects the rights of staff, volunteers, partners, client and any other individuals it comes into contact with;
- Is open about how it stores and processes individuals' data;
- Protects itself from the risks of a data breach.

Information Security

The protection of data relates to all data provided by individuals as well as data shared by external agencies with Thames Valley Partnership.

Technical Terms

Data – information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data Subjects – all living individuals about whom a business holds personal data.

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

Data Controllers – the people who, or organisations which, determine the purposes for which, and the manner in which, any personal data is processed.

Data Users – employees whose work involves processing personal data. Data users must protect the data they handle in accordance with the data protection obligations and policies of a business.

Data Processors – any person or organisation that is not a data user that processes personal data on behalf of a business.

Processing – any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending retrieving, using, disclosing, erasing or destroying it.

General Data Protection Regulations (GDPR) – the UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that Thames Valley Partnership follows its Data Protection Policy and complies with GDPR. The Data Protection Officer and Partnership Director are responsible for ensuring Thames Valley Partnership meets its obligations. The Data Protection Officer is Neil Owen and may be contacted via email at admin@thamesvalleypartnership.org.uk.

Information Commissioner – The UK Information Commissioner is responsible for implementing and overseeing current legislation.

People, Risks and Responsibilities

Everyone who works for, or with, Thames Valley Partnership is responsible for ensuring data is collected, stored and handled appropriately. Individuals specifically working with such data must ensure that it is handled and processed in line with this policy and GDPR. Any individuals with concerns around the protection of data e.g. a data breach, should bring this to the attention of the Data Protection Officer immediately. This policy applies to all data that Thames Valley Partnership holds relating to identifiable individuals. This may include, but is not limited to:-

- Names of individuals
- Data of Birth;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- Sensitive information;
- Any other information relating to individuals.

Data Protection Controller

Thames Valley Partnership determines for what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds, or is likely to hold, and the general purposes that this data will be used for.

Thames Valley Partnership will adhere to the Principles outlined in the GDPR and will, through appropriate management, ensure the strict application of controls:-

- To comply fully with conditions regarding the collection and use of information;
- To meet its legal obligations to specify the purposes for which information is used;
- To collect and process appropriate relevant information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements;
- To ensure that there is a lawful basis for collecting and processing data;
- To ensure the quality and accuracy of information used;
- To ensure that the rights of people about whom information is held can be fully exercised under the GDPR.
- To ensure appropriate technical and organisational security measures are in place to safeguard personal information;
- To ensure data is stored and protected securely and not held any longer than necessary;
- To ensure the secure destruction of all electronic and paper files at the point at which they are no longer required.

Data Collection

Thames Valley Partnership will ensure that data is collected within the boundaries defined in this policy and the GDPR. This applies to data that is collected in person or by completing a form.

When collecting data, Thames Valley Partnership will ensure that the Data Subject clearly understands why the information is needed, what it will be used for, who it may be shared with, how it will be stored, how long it will kept for and how we will dispose of it. Further details are contained within our Privacy Notice.

Thames Valley Partnership will ensure at all times that there is a legal basis for collecting the data. In most cases this will be either under 'contract', as a service delivery provider, on behalf of a government agency or with the explicit consent of the data subject.

Data Storage – Physical Data

When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it. This also applies to data which may be stored electronically but has been printed and is now also available as a hard copy.

Guidelines for physical data:-

- When not required, the paper or files should be kept in a locked drawer or filing cabinet with access only available to those who need it for their work;
- When storing data for *related* individuals these will be locked securely in separate locations e.g. victim and linked offender details will be stored separately to avoid cross reference;
- Paper or printouts containing personal information should not be left where others may have access e.g. printouts should be collected immediately and not left on the printer;
- In circumstances which require paper files to be transported by post these should be double enveloped in plain, inconspicuous packaging with a return address. Related information should be sent as a separate package.
- Data printouts should be shredded and disposed of securely when no longer required. If disposing of such data through a collection bag, this should be securely locked away until collection and should not be left out in the office.
- When taking handwritten notes, personal data should be anonymised or individuals/cases identified by initials/case numbers.

Data Storage – Electronic Data

When data is stored electronically all efforts should be taken to prevent unauthorised access, accidental deletion and malicious hacking attempts.

Using Laptop/Desktop Computers:-

- Staff will be issued with an encrypted laptop/desktop. These generally have inbuilt encryption, but others have an encryption key. Those with an encryption key are responsible for ensuring that the key is stored separately from the laptop when not in use. If the key is lost this must be reported immediately to the TVP office.
- All computers and laptops should be password protected by strong passwords which are changed regularly (at least every 90 days) and never shared between employees (except within the core team) or with an external party;
- Unattended computers should always be screen locked;
- Laptops should always be locked away when not in use
- Individual documents containing personal or sensitive data should be password protected;
- Employees must not store personal data on removable devices (e.g. CD, DVD, Memory Stick).
- Data should only be uploaded to an approved cloud based computing service; e.g. case management software, payroll software etc.
- Data should be backed up frequently. These backups should be tested regularly, in line with the company's standard backup procedures;

- All servers and computers containing data should be protected by approved security software and a firewall;
- Data will only be accessible to those who need it for their work;
- Personal data should not be shared informally. In particular, it should never be sent by email as this form of communication is not secure (unless via the established secure mail route e.g. CJSM);
- Those working remotely will not access data using an unsecure network; e.g. coffee shop, hotel etc.
- All personal and company data should be non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party;
- Temporary/cached files should be deleted by individuals from their computer/laptop on a regular basis (this should be done at least weekly).

Using Email:-

In addition to their normal business email address, employees dealing with sensitive information/ client casework will be issued with secure email e.g. a Criminal Justice Secure Mail (CJSM) account, usually accessed through a secure website.

- Secure email e.g. CJSM must be used when sending sensitive and/or personal information.
- Secure email must only be accessed on a TVP issued encrypted device on a secure WIFI/internet connection.
- Secure mail must never be accessed on unencrypted or personal laptops/desktops.
- Secure email must never be accessed via an unsecured network e.g. a coffee shop.

If, on very rare occasions, it's absolutely necessary to use personal/unsecure emails for sending personal data, individuals/cases should be anonymised or referenced by initials/case numbers.

Individuals are responsible for ensuring that Email history and Contact details held in Microsoft Outlook are regularly purged.

Emails kept for any purpose should not be kept for any longer than is absolutely necessary for that purpose.

Using Mobile Phones: -

Mobile phones must not be used for secure email.

Personal data held on mobile phones should be kept to an absolute minimum and then must be anonymised and referenced by initials/case numbers.

Mobile phones should not be used on unsecured WIFI networks, such as coffee shops etc. to check emails or to access emails through the internet.

Personal data and/or contact details kept on mobile phones for any purpose must not be kept for any longer than is necessary for that purpose. This data must be regularly purged.

Guidance for Volunteers/Associates

Individuals using their own personal PC, email, mobile phone or any other electronic device to complete work for Thames Valley Partnership are responsible for ensuring that they do not save any personal or sensitive information relating to anyone associated with TVP, including its clients.

Personal data must not be visible to, or shared with, family members or anyone else.

Where it is necessary to record personal data on physical (e.g. paper) or electronic media this must be anonymised or referenced by initials/case numbers at all times.

Personal data and/or emails should not be kept for any longer than is absolutely necessary for that purpose.

Paper/hard copy information should only be carried outside of the office where absolutely necessary and should be returned to the office for safekeeping/shredding when no longer required. When in transit It must be carried in appropriately secure wrapping/case and never left unattended e.g. in a coffee shop or car. If temporarily kept at home it should be securely locked away and never left where it can be viewed by family members/visitors. Those carrying paperwork must be mindful at all times of the potential risk of loss/theft and must be vigilant and execute proper care and attention.

Email history and/or details of Contacts held in Email systems such as Microsoft Outlook, relating to Thames Valley Partnership, must be regularly purged.

Temporary/cached files should be regularly deleted from personal computers – at least on a weekly basis.

Hand written case notes must be returned to the office after use and securely destroyed.

Data Accuracy

Thames Valley Partnership is required to take reasonable steps to ensure data is kept accurately and up-to-date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up-to-date as possible.

Thames Valley Partnership will ensure:-

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets;
- Staff should take every opportunity to ensure data is updated;
- It is easy for data subjects to update the information the Partnership holds about them e.g. through prompts on staff and volunteer expenses forms;
- Electronic and paper files are deleted and disposed of securely at the point at which they are no longer required.

Disclosure

Thames Valley Partnership may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are, however, circumstances where the law allows Thames Valley Partnership to disclose data (including sensitive data) without the Data Subject's consent. These circumstances include:-

1. When carrying out a legal duty or as authorised by the Secretary of State;
2. When protecting the vital interests of the individual;
3. When the individual has already made the information public;
4. When conducting any legal proceedings, obtaining legal advice or defending any legal rights;
5. When monitoring for equal opportunities purposes i.e. race, disability, religion etc.;
6. When providing a confidential service where the individual's consent cannot be obtained or where it is reasonable to proceed without consent e.g. where we would wish to avoid forcing stressed or ill individuals to provide consent signatures.

The Data Controller will ensure any request under such circumstances is legitimate, seeking assistance from the Board and via external advice where necessary.

Detailed guidelines to assist staff in the execution of this policy is available from the Data Protection Officer on request.

An Individual's Rights under GDPR

All individuals who are the subject of personal data held by Thames Valley Partnership have rights under GDPR. These include:-

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information;
- The right to restrict processing in certain circumstances;
- The right to rectification of information which is regarded as incorrect;
- The right to erase information;
- The right to data portability;
- The right to object;
- The right to lodge a complaint

Requests by individuals to exercise their rights should be made by email or post to the Data Protection Officer.

The Data Protection Officer will always verify the identity of anyone making an access request before handing over any information (e.g. by checking date of birth etc.) to ensure this matches the records held. If an access request is made via a third party the Data Protection Officer will consider whether the third party has the consent of the Data Subject and will then act accordingly. Requests will be responded to within one month and will generally be free of charge unless the request is unfounded,

excessive or repetitive in which case a fee of £10 per request will be charged to the individual requesting access.

Review of Policy

This policy will be reviewed on an annual basis by the Data Protection Officer to ensure it remains up-to-date and reflects the needs and practices of the organisation.

Signed: _____
Reviewer

Date of Review: _____