Data Protection and Privacy Policy

Tru is a trademark of The Truprint Group.

Introduction:

The Truprint Group and or its affiliated projects such as Tru needs to gather and use certain information about individuals and store the data accordingly.

This will include customers, subscribers, suppliers, employees, volunteers, business contacts, sponsors and other people the organisation may work with or need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Summary:

Part 1: Definitions

Employee: This is a paid member of the Truprint staff, where by a formal contract will be signed. A job description and all other necessary will be supplied.

Volunteer: This is a non-paid member of the Truprint team, where by a volunteer agreement may be signed.

Staff: For the purpose of this document only, the word "staff" will refer to both employees and volunteers.

Part 2: Why this Policy Exists

The data protection policy will comply with the data protection law and follow good practice. The policy protects the rights of staff, customers and any other party involved, and informs everyone about how it is stored. It is also in place in case there is a data breach, as it includes the procedures for a breach.

Part 3: Data Protection Law

The Data Protection Act of 1998 was put in place to keep personal information safe, it describes how organisations including The Truprint group must collect, handle and store personal information. These rules apply to all forms of storage, this could be on paper or electronically.

As well as being collected and used fairly, it must be stored safely and not disclosed unlawfully.

The main principles of the of the Data Protection Act are:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

Part 4: People Risks and Responsibilities

Policy scope - This policy applies to:

1. The director of The Truprint Group
2. All future branches/projects of The Truprint Group
3. All staff and volunteers of the The Truprint Group
4. All suppliers, sponsors and other people working on behalf of the Truprint company

It applies to all the data held by The Truprint Group, relating to individuals, even if that information technically falls outside of the Data Protection Act 1998 and General Data Protection Regulation (GDPR). This includes, names, numbers, addresses and any other contact or personal information relating to the individual. It also includes data known as sensitive data. This can include, religion, ethnic origin, sexual orientation etc.

Part 5: Data Protection Risks

This policy helps to protect The Truprint Group from some data security risks including:

1. Breaches of confidentiality. For instance, information being given out inappropriately.
2. Failing to offer choice. For example, all individuals should be free to choose how the company uses data relating to them.
3. Repetitional damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Part 6: Responsibilities

Everyone who works for or with The Truprint Group has some responsibility for ensuring data is collected, stored and handled appropriately.

Any data should be kept between the company and for no reason should be given out to a third party, shared or displayed unlawfully unless has been consented for example an interviewee. These people have key responsibilities regarding personal data;

The company director **Ellis Jackson,** is ultimately responsible for:

1. Ensuring that the The Truprint Group meets its legal obligations.
2. Arranging data protection training

3. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
4. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.

The data protection officer **Ellis Jackson**, is responsible for:

1. Keeping the director updated about all data protection risks, issues and responsibilities.
2. Keep the Data Protection Policy updated.
3. Reviewing data protection procedures and related policies, in like with an agreed schedule
4. Handling data protection questions and queries
5. Requests from individuals to see information stored about them.

The marketing or business support manager **Ellis Jackson**, is responsible for:

1. Approving any data protection statements attached to communications such as emails and letters.
2. Addressing any data protection queries from outside sources.
3. Working with staff to ensure marketing initiatives abide by data protection principles

Part 7: General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work. For example, contacting potential business partners/sponsors or subscribers.

Data should not be shared informally. If a staff member wishes to obtain personal data, it should be requested from the data protection officer or company director.

Staff should make sure that if setting up or are given passwords or access to any files on the system, the passwords must never be shared.

Personal data should not be disclosed to unauthorised people, either within the company or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Any customer that has subscribed to the company or any viewer on site if leaving contact details, needs to have consented before any emails and information can be sent to them.

Staff should request help from the company director or data protection officer, if they are unsure about any aspect of data protection.

Part 8: Data Storage

Staff are encouraged to work from our website and or One Drive at all times, this is to ensure data is protected and secure and that no work is saved onto personal drives. Our website and One Drive are a secure, restricted space where by only staff have access to and is automatically backed up and password protected.

These guidelines apply to electronic data:

1. Data should be protected by strong passwords that are changed regularly, and never shared.
2. If data is stored on removable media such as a USB stick, it should be locked away safely.

3. Data should only be stored on designated drives and servers and uploaded on to approved cloud computing services.
4. Data should be backed up frequently.
5. Data should never be saved directly to devices such as mobile phones, tablets and some laptops. Unless they are deleted immediately after converted to the correct location.
6. All servers and computers containing data should be protected by approved security software and a firewall.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

Data stored on paper, or electronic data that has been printed, when not required should be kept in a locked drawer or filing cabinet. The paper should not be left where unauthorised people can see it and if the data is no longer required, it should be shredded.

Part 9: Use of Data

1. When working with personal data, staff should ensure the screens of laptops are locked when left unattended.
2. Personal data should never be shared informally, and not by any form of communication which is not secure.
3. Personal data should never be transferred outside of the European Economic Area.
4. Staff should never save copies of personal data to their own computers.

Part 10: Staff Names and Photographs

The Truprint Group and it's brands or projects may post from time to time, pictures, videos, staff names and role descriptions through outlets such as our websites, social media accounts or any other other outlets owned by The Truprint Group, it's brands or projects for the purpose of credits, staff promotional announcements or other similar purposes.

If you do not wish for us to do this please inform us via www.tru.uk/contact in writing before any work is published or as soon as you have read this document.

Part 11: Data Accuracy

The law requires that The Truprint Group to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all staff who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places as necessary, staff should not create unnecessary additional data sets.

Staff should take every opportunity to ensure data is updated. For instance, by regular emails to subscribers confirming their details.

The Truprint Group will make it easy for data subjects to update the information the The Truprint Group holds about them. For instance, via the company website.

Data should be updated when inaccuracies are discovered. An example would be a telephone number no longer in use.

It is the company director's responsibility to ensure marketing and other data bases are checked every six months.

Part 12: Subject Access Requests

All individuals who are the subject of personal data held by The Truprint Group are entitled to:

1. Ask what information the company holds about them and why
2. Ask how to gain access to it
3. Be informed how to keep it up to date
4. Be informed how the company is meeting the data protection obligations.

If an individual contact's the company requesting this information, this is called a subject access request.

These requests should be made by a formal email, addressed to the data controller.

This information will be provided within **14 days**.

The data controller will need to verify the identity of anyone making a request.

Data can also be disclosed to law enforcement agencies, if this is requested the data controller must make sure that they are legitimate. These can be made without the consent of the individual concerned.

Part 13: Purpose and Processing

It is required we keep all staff data secure, as well as the obvious reasons we store information. The Truprint Group's staff data is kept for the purposes of:

1. For your line manager to be able to contact you regarding work completed, shifts etc.

2. Your NDA's, contracts and consent forms so staff follow The Truprint Group policies and regulations.

We store customer information if they have subscribed to The Truprint Group's mailing list, memberships, and subscriptions and have agreed to any necessary privacy and data protection policies for the purpose newsletters, advertising, updates, invites and offers and to make sure that they are receiving relevant information regarding their subscription.

Part 14: Disciplinary Procedures

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action.

Updated: 1.4.20

Authorised by: Ellis Jackson