Tarff Valley Ltd
Data Protection Policy

Introduction

Our Data Protection Policy sets out our commitment to protectiong personal data and how we implement that commitment with regards to the collection and use of personal data.

We are committed to:

- Ensuring that we comply with the eight data protection principles, as listed below
- Meeting our legal obligations as laid down by the Data Protection Act 1998
- Ensuring that data is collected and used fairly and lawfully
- Processing personal data only in order to meet our operational needs and fulfil legal requirements
- Taking steps to ensure that personal data is up to date and accurate
- Establishing appropriate retention periods for personal data
- Ensuring that data subjects rights can be appropriately exercised
- Providing adequate security measure to protect personal data
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- Ensuring that all staff are made aware of good practices in data protection
- Providing adequate training for all staff responsible for personal data
- Ensure that everyone handling personal data knows where to find further guidance
- Ensuring that queries about data protection, internal and external to the company, is dealt with effectively and promptly
- Regularly reviewing data protection procedures and guidelines within the company

Data protection principles

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose and those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- Personal date shall be processed in accordance with the rights od data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing or personal data

Document retention

We will ensure that the storage and retention of all forms of client/customer information and data complies with our requirements under the Data Protection Act 1998.

This will cover what type of information we are required to keep, in what format we keep it and for how long.

In this policy the description 'document' covers any information that is retained in a paper format, electronically input, scanned documents and documents saved by other means such as on disc.

All scanned or electronically saved documents are accepted as evidence therefore we must ensure that we continue to have access to the data and that we have a robust backup procedure in place so that copies can be retrieved when required. We must also ensure we continue to have access to any appropriate hardware or software so that as our information systems develop we retain the technology to access redundant data storage formants or upddate the format in which the data is stored.

Terms and Conditions

The details of our terms and conditions sets out our data protection principles to ensure our clients/customers are aware of our responsibilities and their responsibilities in relation to the Data Protection Act 1998 and any documents and information we hold.

Internal procedures

Our nominated officer is responsible for data protection compliance and ensures that we act in accordance with the principles of the Data Protection Act 1998.

We ensure that, at the end of each working day, all documents and files are locked away in a safe and retrievable place.

Due diligence is exercised at all times within the IT equipment and systems ensuring the safety of client /customer data and any other sensitive information and our office security is designed to ensure client/customer personal data protection is maintained.

Staff are made aware of our internal procedures and annual training is given to all staff to ensure they are fully aware of their role so that we comply with data protection principles. All staff training will be documented.

CCTV Image storage, viewing and retention

Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified. Access to live images is restricted to the CCTV operator unless the monitor displays a scene which is in plain sight from the monitored location. Recorded images can only be viewed in a restricted area by approved staff. The recorded images are viewed only when there is suspected criminal activity and not for routine monitoring of staff or visitors unless the camera(s) are installed to monitor the safe movement of persons through a designated area. Tarff Valley reserves the right to use images captured on CCTV where there is activity that cannot be ignored such as criminal activity, potential gross misconduct, or behaviour which puts others at risk. Images retained for evidential purposes will be retained in a locked area accessible by the system administrator only. Where images are retained, the system administrator will ensure the reason for its retention is recorded, where it is kept, any use made of the images and finally when it is destroyed.

Neither the Data Protection Act nor the Information and Records Management Society prescribe any specific minimum or maximum periods which apply to CCTV recorded images. Images are not retained for longer than is necessary. Once the retention period has expired, the images are removed or erased.

Disclosure

Disclosure of the recorded images to third parties can only be authorised by the data controller. Disclosure will only be granted:

- If its release is fair to the individuals concerned.

- If there is an overriding legal obligation (eg information access rights).

- If it is consistent with the purpose for which the system was established.

All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented. NB: Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

Do:

- seek to comply with the principles of the Data Protection Act
- recognise that the Act applies to paper and electronic files
- think of data held about other individuals in the same way as if it were your data
- get permission to hold data or establish if consent has already been given, where needed
- be particularly careful when dealing with sensitive personal data: eg data concerning race or ethnic origin, political opinion, religious belief, sexual life, criminal offences, trade union membership, health
- hold data about individuals only when it is necessary and for no longer than is necessary
- endeavour to ensure that data is accurate and kept up to date, where necessary
- respect confidentiality
- discard personal files as confidential waste
- bear in mind, when writing documents, that individuals have the right to see their files
- realise that emails may be retrieved and revealed to those about whom they are written
- pass all Subject Access Requests to Ian Billings

Don't:

- worry about the complexities of the Act - concentrate on the principles
- reveal data to third parties without the data subject's explicit permission eg telephone numbers / email addresses
- hold sensitive data about an individual without the data subject's explicit consent
- put data about individuals on the Internet without permission
- send personal data outside Tarff Valley
- leave personal data insecure
- take personal data home without being acutely aware of the need for security
- part with computers without ensuring they are cleared of personal data
- use email for confidential communications
- use data held for one purpose for a different purpose without seeking permission to do so