Introduction

The company considers the data and physical security of its people, customers and suppliers to be of vital importance. All colleagues must therefore be alert and conscientious in all matters relating to data and site security. This policy is reviewed by management every 2 years or upon legislation change.

Personal property

Wherever possible, try to avoid bringing valuables into the workplace.

You should look after your personal belongings as the company cannot accept responsibility for damage to, or the theft/loss of personal belongings. If you do lose, damage or have personal property stolen whilst on the company premises, you should inform your manager immediately.

Company and client property

You are responsible for all company property including, but not limited to, any money which you handle and any uniform or protective clothing which is provided for your use.

No items of company or client property may be removed from the company or client premises without your manager's or the client's authorisation. If you are found to have taken or removed company or client property from the premises (even if the item in question has apparently been discarded), you may be liable to legal action, in addition to action under the Disciplinary procedure for gross misconduct. This may lead to your dismissal without notice and without payment in lieu of notice.

No unauthorised visitors are allowed on site and if you see anyone unknown to you walking around the site, please report this to management immediately.

You are never to pass any site keys or keycodes to anyone not authorised to have them.

Data protection

We are committed to being transparent about how we collect and use personal data and in meeting our data protection obligations. This section of the policy explains our commitment to data protection, your rights and your responsibilities in relation to it.

The government use certain definitions in relation to data protection, so to ensure you understand what they mean when we use them in this policy, we have clarified them below:

- "Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that I made of this data. 'Special categories' of personal data refers to the information that is subject to higher levels of protection because it is more sensitive. The regulation categorises this as health, race, religion, sexual orientation, ethnic origin, trade union membership, sex life, genetic & biometric data, and political opinions.

  If we ever needed to process special categories of data, we would do so in accordance with the more stringent guidelines.

- "Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles

We (the company) process your personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner
- We collect personal data only for specified, explicit and legitimate purposes
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing

- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- We keep personal data only for the period necessary for processing
- We adopt appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

We tell you the reasons for processing your personal data, how we use such data and the legal basis for processing in our privacy notice. HR related data will not be shared to third parties except as set out in the privacy notice for things like enabling payroll to pay you, pensions to be calculated and accrued accurately etc.

If we need to process special categories of personal data (such as if you are seriously ill) or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with the law.

We update your HR related personal data promptly, however this can only be done if you tell us your information has changed or is inaccurate. Personal data gathered during your employment is held in your individual personnel file (P drive, in hard copy or electronic format, or both), and on HR systems. The period for which we hold HR related personal data is in line with employment law.

Customer and supplier personal data are stored on the K drive, sage and Tharstern system.

The organisation keeps a record of its processing activities in accordance with the requirements of General Data Protection Regulation (GDPR).

Your rights

As described above, we process personal data in order to carryout certain activities like pay our staff or fulfil orders. In the governments language you are known as a data subject and as such you have a number of rights in relation to your personal data as outlined below:

Subject access requests:

You have the right to make a subject access request in relation to your data. If you make a subject access request, we follow government guidelines on what we need to tell you, which is explained below:

- Whether or not your data is processed and if so why
- The categories of personal data concerned
- The source of the data (if it is not collected from you)
- To whom the data is or may be disclosed, including the recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers
- For how long your personal data is stored (or how that period is decided)
- Your rights to rectification or erasure of data, or to restrict or object to processing
- Your rights to complain to the Information Commissioner if you think we have failed to comply with your data protection rights
- Whether or not we carry out automated decision making and the logic involved in any such decision making

We will also provide you with a copy of the personal data undergoing processing. This will normally be in electronic form. If you require additional copies, we will charge a fee based on the administrative cost of providing the additional copies.

To make a subject access request you should send an email to your manager or enquiries@technoprint.net (for non-employees), who will ensure that it is sent to the right person. In some cases, we may need to ask for proof of identification before the request can be processed. We will normally respond to requests within a period of one month from the date it is received. In some cases, such as where we process large amounts of an individual's data, we may respond within three months of the date the request is received. We will write to you within one month of receiving the request to tell you if this is the case.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If you submit a request that is unfounded or excessive, we will let you know that this is the case and whether we will respond to it.

Data protection principles

You have several other rights in relation to your personal data such as:

- Rectify inaccurate data
- Stop processing or erase data that is no longer necessary for the purposes of processing
- Stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data)
- Stop processing or erase data if processing is unlawful
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the organisation's legitimate grounds for processing data
- You are responsible for helping us to keep data up to date. You should let us know if your data changes, for example if an individual moves to a new house or changes bank details

Data security principles

You may have access to the personal data of individuals and of our customers and clients in the course of your employment (contract, volunteer period, internship or apprenticeship). Where this is the case we rely upon you to help meet our data protection obligations to our people and to customers and clients.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes
- Not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation
- To keep data secure by:
    - Ensuring all laptops and computers are kept updated with suitable anti-virus, anti-malware, spam filter and firewall protection. Our IT company ITG are responsible for updates, backups and IT security. Our backup systems are challenged on a quarterly basis and recorded under entropy schedule
    - Not answering suspicious looking emails
    - Store files in official company storage locations
    - Do not use you work equipment for personal use or your personal equipment for work use
    - Don't use administrator accounts for your day-to-day use
    - Don't divulge your password to anyone
    - Lock your computer when leaving it unattended
    - Software systems such as Tharstern shall be set to automatically time out after a period of 15 minutes of non-use
    - Not to remove personal data or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection, and do not leave unattended or in a vehicle)
    - To report data breaches to your manager, immediately upon identifying them

<u>Password policy:</u>

- Change default passwords and PINs on computers, phones and all network devices – such as those created for new employees or to protect new systems when set up – as quickly as possible.
- Don't share your password with other people or disclose it to anyone else.
- Don't write down PINs and passwords next to computers and phones.
- Employees should choose passwords that are at least 12 characters long, but no longer than 15 and contain a combination of upper-case and lower-case letters, numbers/symbols. These requirements will be enforced with software when possible.

- All passwords should be reasonably complex and difficult for unauthorized people to guess.
- Employees should use common sense when choosing passwords. Avoid basic combinations that are easy to crack. For instance, choices like “password,” “password1” and “Pa$$w0rd” are equally bad from a security perspective.
- Make your password memorable and specific: Choose something only you know and that you’ll be sure to remember.
- Choose uncommon words/phrases separated by numbers/symbols (e.g. **Field65-Medic** or **Wall87!Goggles** – this helps to keep the password memorable to avoid writing it down, but still complex enough.
- If you believe your password may have been compromised, please immediately change the password and report the incident to your manager.

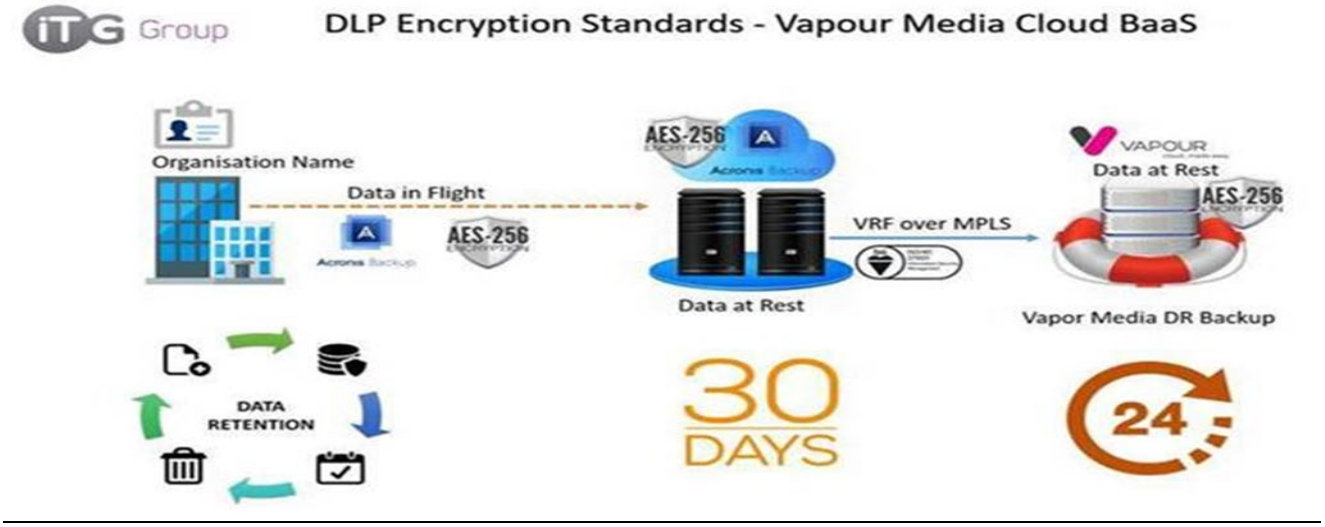
Backup, disaster recovery and continuity:

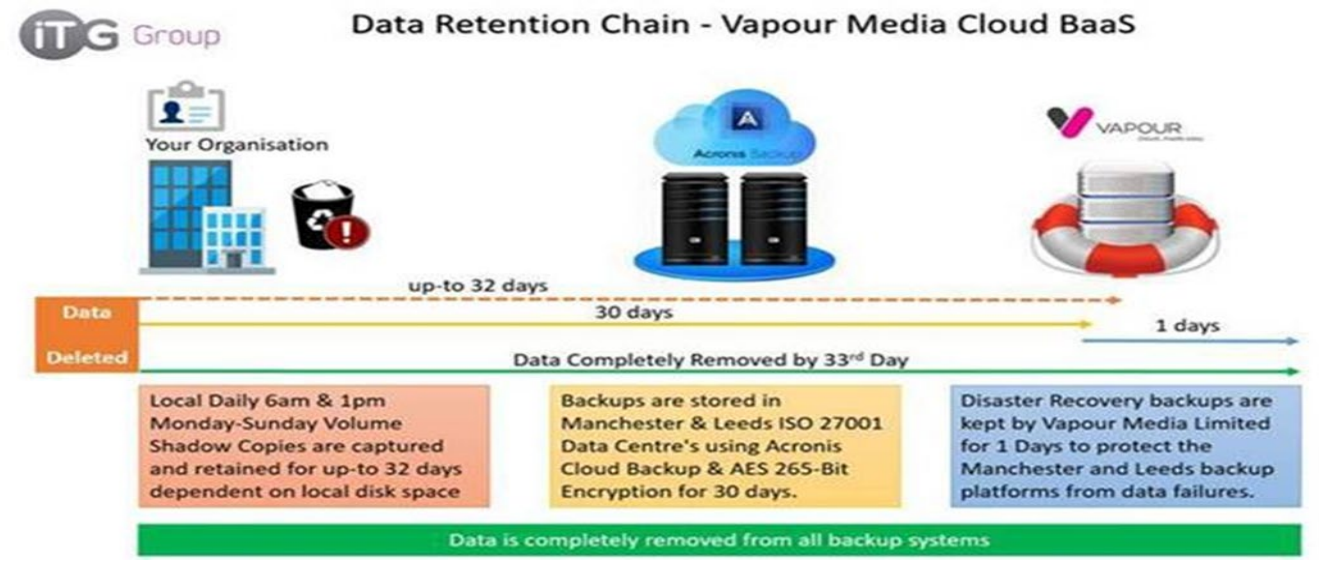
Backups are controlled by our external IT company ITG.

The managed, cloud backup involves ‘selected data areas’ backups to an ISO27001 Data Centre in Manchester where up-to 30-backups retention remains then the latest backup is then replicated to an ISO27001 Data Centre in Leeds once nightly for ITG’s services Disaster Recovery.

All data is encrypted with 256-bit AES Encryption during the backup process, this data is encrypted in transit from Technoprint to the data centre and at rest in the data centre.

The data streams to the data centre are also SSL encrypted separately.





The following servers are protected:

Tech-SVR01 (Role: Domain Controller | Primary Data Storage)

Retention: 30-backups

Included.

D:\Shares\Artwork\

D:\Shares\Company\

D:\Shares\Line50\

D:\Shares\Personnel Records\

D:\Shares\SQLBackup\ (Local SQL backup repository mentioned below.)

D:\Shares\Users\

Excluded.

D:\Shares\Software

Tech-SVR02 (Role: Terminal Server)

Retention: 30-backups

Included.

C:\Users\

Excluded

N.A

Tech-SVR03 (Role: Applications – Primo/Goldmine)

Retention: 30-Days

Included.

C:\Tharstern\

Excluded

N.A

Microsoft SQL Server on - Tech-SVR03 (Backed up Locally to TechSVR01 D:\Shares\SQLBackup\)

Retention: Full 2 Months Incremental 31-Days

Included Databases.

- System Databases
- GoldMine
- ReportServer
- ReportServerTempDB
- Technoprint
- TharData

Entropy audit schedule AUD00037 controls the prompting of quarterly challenges of the backup system. When entropy has scheduled an audit, ITG shall be contacted to request a backup challenge; the provide results shall then be saved and attached to the audit record.

Data breaches

If we discover that there has been a breach of personal data that poses a risk to your rights and freedoms, we will report it to the Information Commissioner within 72 hours of discovery. We record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

Privacy notice

The company is aware of its obligations under the General Data Protection Regulation (GDPR) and domestic data protection legislation and is committed to processing your data securely and transparently. This privacy notice sets out, in line with the current data protection obligations, the types of data that we hold on our employees and customers. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

Data controller details

The company is a data controller, meaning that it determines the processes to be used when using your personal data.

Data protection principles

In relation to your personal data, we will:

- Process it fairly, lawfully and in a clear, transparent way
- Collect your data only for reasons that we find proper for the course of your employment or our partnership, in ways that have been explained to you
- Only use it in the way we have told you about
- Ensure it is correct and up to date
- Keep your data for only as long as we need it
- Process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed

Types of data we process

We hold many types of data about you:

- Your personal details including your name, address, date of birth, email address, phone numbers
- Your photograph
- Gender
- Marital status
- Dependents, next of kin and their contact numbers
- Medical or health information including whether or not you have a disability
- Information used for equal opportunities monitoring your sexual orientation, religion or belief and ethnic origin
- Information included on your CV including references, education history and employment history
- Documentation relating to your right to work in the UK
- Driving licence

- Bank details
- Tax codes
- National insurance number
- Current and previous job titles, job descriptions, pay grades, pension entitlement, hours of work and other terms and conditions relating to employment with us
- Letters of concern, formal warnings and other documentation with regard to any disciplinary proceedings or, in the case of workers, confirmation of other discussions about your conduct
- Initial performance information including measurements against targets, formal warnings and related documentation regarding capability procedures, appraisal forms or in the case of workers, confirmation of other discussions about your performance
- Leave records including annual leave, family leave, sickness absence etc
- Details of your criminal record
- Training details
- CCTV footage

How we collect your data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment or customer onboarding exercise, where we will collect the data directly from you. This includes the information you would normally include in a CV or recruitment cover letter, or notes made by our recruitment officers or Key Account Manager during a recruitment interview or order estimating. Further information will be collected directly from you when you complete forms at the start of your employment/engagement, for example your bank details. Other details may be collected directly from you in the form of official documentation such as driving licence, passport to other right to work evidence.

In some cases we will collect data about you from third parties such as employment agencies or former employers or suppliers, when gathering references or credit reference agencies.

Personal data is kept in personnel files or within the Company's HR and IT systems.

Why we process your data

The law only lets us process your data for certain reasons:

- In order to perform the employment or sales contract we are party to
- In order to carry out legally required duties
- In order for us to carry out legitimate interests
- To protect your interest
- When something is done in the public interest
- Where we have obtained your consent

All the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to:

- Carry out the contract we have entered into with you
- Ensure you are paid

We also need to collect your data to ensure we comply with legal requirements such as:

- Ensuring tax and National Insurance are paid
- Carrying out checks in relation to your right to work in the UK
- Making reasonable adjustments for disabled individuals

We also collect data to that we can carry out activities which are in the legitimate interest of the company. We have set these about below:

- Making decisions about who to offer initial employment/engagement to, and subsequent internal appointments/promotions etc
- Making decisions about salary and other benefits
- Providing contractual benefits to you
- Maintaining comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- If you are an employee, effectively monitoring both your conduct and your performance and to undertake procedures with regards to both of these if the need arises
- If you are an employee, offering a method of recourse for you against decisions made about you via a grievance procedure
- Assessing training needs
- Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken including the making of reasonable adjustments
- Gaining expert medical opinion when making decisions about your fitness for work
- Managing statutory leave and pay systems such as maternity leave and pay etc
- Business planning and restructuring exercises
- Dealing with legal claims made against us
- Preventing fraud
- Ensuring our administrative and IT systems are secure and robust against unauthorised access

Special categories of data are data relating to your:

- Health
- Sex life
- Sexual orientation
- Race
- Ethnic origin
- Political opinion
- Religion
- Trade union membership
- Genetic and biometric data

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- You have given explicit consent to the processing
- We must process the data in order to carry out our legal obligations
- We must process data for reasons of substantial public interest
- You have already made the data public

We will use your special category data:

- For the purposes of equal opportunity monitoring
- In our sickness absence management procedures
- To determine reasonable adjustments

We do not need your consent if we use special categories of personal data in order to carry out legal obligations or exercise specific rights under employment law, however we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. The data will usually be collected at the recruitment stage, however, may also be collected during your employment. We rely on the lawful basis to process this data, if required for a job; if this is the case we will contact you.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract with us. If you do not provide us with the data needed to do this, we will be unable to perform those duties, e.g. ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment/engagement with us in relation to our legal obligations if you do not provide us with the information e.g. confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check, confirming your company is legitimate.

Sharing your data

Your data will be shared with colleagues within the company where it is necessary for them to undertake their duties. This includes, for example, line managers for the management of employees, HR for maintaining personnel records and payroll/accounts for administering payment under your contract.

We may share your data with third parties in order to pay pensions, wages and administer HR support and marketing.

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with legal obligation upon us. We do not share your data with bodies outside of the European Economic Area.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such. Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with current data protection requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it, which will be at least the duration of your employment or partnership with us, though in some cases we will keep your data for a period after this has ended. Retention periods can vary depending on why we need to keep your data.

Automated decision making

No decision will be made about you solely based on automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- The right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- The right of access. You have the right to access the data that we hold on you. To do so, you should make a Subject Access Request. You can read more about this in the data section of this policy (above)
- The right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- The right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- The right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct.
- The right to portability. You may transfer the data that we hold on you for your own purposes
- The right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interest
- The right to regulate any automated decision making and profiling of personal data. You have a right, not to be subjected to automated decision making in a way that adversely affects your legal rights

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent, however in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact your manager or enquiries@technoprint.net

Making a complaint

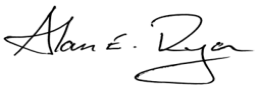
The supervisory body in the UK for data protection matters is the Information Commissioner's Office (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

Data Protection Officer

The company's Data Protection Officer is Jacqui Morris.

Failing to observe these requirements may amount to a disciplinary offence which will be dealt with under the disciplinary section of the handbook. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could result in dismissal without notice.

Signed:



Alan Ryan

Managing Director

Employee commitment

I agree to follow the Technoprint data and site security policy

Signed: _____ Date: _____