BARTRUMS
HAULAGE AND STORAGE LTD

Langton Green, Eye, Suffolk, IP23 7HN
Telephone: 01379 870693
Fax: 01379 870942
Email: info@bartrums.com
www.bartrums.com

Data Protection Policy

Data Protection and Information Management

Introduction

Bartrums will use the term “Information Management‟ to describe the rules on handling information. This term covers issues such as Data and Quality (making sure information is accurate and available), Records Management (a systematic method of recording information), Data Protection (which places obligations on how personal information is used), confidentiality and security.

Confidentiality and security measures overlap and support each other. Information Management covers all information – confidential and non-confidential within the Company.

The 1998 Data Protection Act was passed by Parliament to control the way information is handled and to give legal rights to people who have information stored about them. Other European Union countries have passed similar laws as often information is held in more than one country.

The Data Protection Act 1998. The Data Protection Act (DPA) gives individuals the right to know what information is held about them, and provides a framework to ensure that personal information is handled properly.

The Company holds 'Personal and Sensitive Personal Information' about our customers and employees. The details are names, addresses, dates of birth, NI numbers and related information about physical or mental health condition.

Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties.

Safeguarding such a large amount of this information kept in a lockable area but information is not obtained simply to store in locked rooms. The information is required wherever it is needed sent and received by teams across the Company as required, with training providers and the accounting purposes.

We must all follow rules on data protection as our company stores or uses personal information.
This applies to information kept on staff, customers and account holders, eg when you:

- recruit staff
- manage staff records
- market services
- use CCTV

This could include:

- keeping personal addresses on file
- recording staff working hours
- giving delivery information to a delivery company

Data protection rules

All employees must make sure the information is kept secure, accurate and up to date.

For example, when you collect someone's personal data you must tell them:

- who you are
- how you'll use their personal information
- they have the right to see the information and correct it, if it's wrong

Also say if the information will be used in other ways - eg if it may be passed to other organisations.

What Bartrums has to do

Bartrums must:

- tell the Information Commissioner's Office (ICO) how the business uses personal information
- respond to a data protection request, if someone asks to see what information we have about them

Recruitment and managing staff records

- You must keep any data you collect on staff secure - eg lock paper records in filing cabinets or set passwords for computer records.
- Only keep the information for as long as you have a clear business need for it, and dispose of it securely afterwards (eg by shredding).

Recruiting staff

- You must give the name of your business and contact details (or those of the agency) on job adverts.
- Only collect the personal information you need on application forms, and don't ask for irrelevant information, like banking details.

Example

You will usually only have to ask about motoring offences if driving is part of the job. Only keep the information for recruitment - eg don't use it for a marketing mailing list.

Keeping staff records

Make sure only appropriate staff, with the right training, can see staff records, and store sensitive information (eg about health or criminal records) separately.

Example

- Don't let managers access a worker's sickness record if they only need to see a simple record of their absences.
- If you're asked to provide a reference, check the worker or ex-staff member is happy for you to do so.
- Letting staff see their records
- Your staff have the right to ask for a copy of the information you hold about them.
- This includes information about grievance and disciplinary issues.
- You must respond to their request within 40 days.
- You may be able to withhold some information when responding to a request if the information concerns someone else - eg you need to protect someone who's accused them of harassment.
- Staff can complain if they think their information is being misused, and you could be ordered to pay a fine or compensation

Monitoring staff at work

You must be able to justify monitoring staff at work, which could include:

- using CCTV
- keeping records of phone calls
- logging their email or internet use
- searching staff or their work areas

Employees have rights at work and if you don't treat them fairly they could:

- take you to an employment tribunal
- complain to the Information Commissioner

You must make them aware that they're being monitored, and why - eg by sending them an email or letter. Also explain your policies on things like using work computers or phones for personal use.

Monitoring staff without their knowledge

You can monitor staff without their knowledge if:

- you suspect they are breaking the law
- letting them know about it would make it hard to detect the crime

Only do this as part of a specific investigation, and stop when the investigation is over.

Using CCTV

- If your business uses CCTV, you must tell people they may be recorded. This is usually done by displaying signs, which must be clearly visible and readable.
- You must also notify the Information Commissioner's Office (ICO) why you're using the CCTV.
- You should control who can see the recordings, and make sure the system is only used for the purpose it was intended for.
- If the system was set up to detect crime, you should not use it to monitor the amount of work done by your staff.

Letting people see CCTV recordings

- Anyone can ask to see images that you've recorded of them. You must provide these within 40 days and inform the individual that a charge up to £10 will apply.
- Data protection rules don't apply if you install a camera on your own home to protect it from burglary.

Criminal Offences - The Data Protection Acts and the Electronic Communications Regulations (SI 336 of 2011) set out the rules with which data controllers must obey. Breaches of these rules sometimes involve offences which are punishable by fines.

Disclosure of personal data which was obtained without authority

The Data Protection Acts deal with the threat to privacy posed by persons who are not data controllers or data processors (or their employees) and who, having obtained unauthorised access to personal information, then disclose it to others. Under section 22 of the Acts, such conduct is an offence. This unauthorised access can occur in various ways. In the case of electronic data the most obvious is "hacking", i.e. obtaining access from a point remote from the computer by electronic means. Unauthorised access can also occur by someone gaining access to a data controller's equipment when the staff are not present. Someone might steal, or take without authority, a diskette or tape or manual file on which data are recorded. Or someone (other than the data controller or his staff) could be in a position to read personal data being shown on the computer screen or to read a printout. But whichever way the unauthorised access takes place, it will be an offence if the person concerned, having gained access, proceeds to disclose to another person the information he or she has accessed.

Obstruction of, or failure to cooperate with, an "authorised officer"

Section 24 of the Data Protection Acts confers certain powers upon an "authorised officer", a person authorised by the Data Protection Commissioner to exercise powers of entry and inspection.

Offences and Penalties – refer to the ICO (Information Commissioners Office) website for more detail

- Offences by data controllers who are required to register
- Offences by any data controllers (not just those who are required to register)
- Offences by employees or agents of registered data controllers
- Offences by data processors who are required to register

- Offences by any data processors (not just those who are required to register)
- Offences by employees or agents of data processors
- Offences by directors etc. of bodies corporate
- Offences by any persons
- Penalties for offences under the Data Protection Act
- Offences by Direct Marketers under S.I. 336 of 2011
- Offences by electronic communications companies under S.I. 336 of 2011
- Penalties for offences under S.I. 336 of 2011

The Information Commissioners Office - Taking Action

There are a number of tools available to the Information Commissioner's Office for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.

The tools are not mutually exclusive. We will use them in combination where justified by the circumstances.

The main options are:

- serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on issues of concern.

Information can be split into 4 types:

Confidential – private information about you; given to somebody who has a duty of confidence (i.e., social care professional); you expect it to be used in confidence – UK law says that personal information is confidential

Personal – all information about a person (name, address, loyalty card details, car you drive, where you went to school, etc) – UK law sets out rules which must be followed by any organisation collecting or using personal information

Sensitive Personal – racial or ethnic origin, political opinions, religious belief, union membership, physical or mental health condition, sexual life, criminal records and health records are sensitive personal information. Other sensitive personal information includes that which could cause damage/distress, i.e. bank/passport details

Anonymous – Carefirst or NHS number, reference number - if information is lost, it is unlikely that person can be identified. Think – could a customer with be identified because of that?

What must be protected?

Confidential information
Common law cases show that a person can take legal action if their confidentiality is broken – this may be by disclosing information to others or failing to protect the information. This covers personal information which a customer gives to our Company (e.g. name and address) - and sensitive personal information (e.g. health details).

Personal information
UK law says that personal information must be protected by adequate security e.g. our names, addresses and dates of birth are held by government when we register to vote and these details must be protected by adequate security.

Sensitive personal information
The same applies to sensitive personal information (the information must be protected by adequate security). The law recognises that the damage or distress caused by a loss or misuse of your sensitive personal information may cause greater damage or distress – which implies even greater protection measures are needed than that required for personal information. It also covers non-health information (e.g. criminal record or ethnic background, sexual orientation) of a job applicant or member of staff who discloses this information to their employer.

Why protect it?

Legal Obligations and Penalties
UK laws demand that we protect these types of information. A person can take legal action if their confidentiality is broken – and a court can decide the amount of compensation to be paid. From April 2010 organisations are liable to a fine of up to £500,000 for reckless use of personal information.

And of course there are other reasons:
Providing a Confidential Service
Customer Trust

What information does not require protection?

Anonymous information – "anonymous" means the person cannot be identified and therefore this is neither personal nor confidential so does not require protection for the purposes of maintaining confidentiality (though there may be other reasons why this should be protected e.g. if it is copyrighted or commercially valuable).

Personal and Sensitive Personal Information in the Public Domain - there are times when personal and sensitive personal information is publicly available and there can be no expectation of confidentiality e.g. newspapers publish the names and address of people convicted of speeding and other crimes; political and religious figures are photographed and named names of senior management and other appointments which are publicly accountable – Managing Director, Operational Directors etc., members of the public, customers or staff who willingly take part in publicity material and give consent for their name and photograph to be used.

Members of the public, customers or staff who take part in publicly accountable forums such as Public Board Meetings, staff in public facing roles – such as social care/support workers, receptionists who deal face to face with members of the public.

Names of Company managers and staff who write letters to customers – we cannot send un-named, unsigned letters. In each of these cases the information disclosed should be limited to what is required e.g. of names on a badge or identity card - not additional information which is not justified.

Confidentiality issues

The duty of confidence regulates the sharing of (disclosure) written and spoken information - but information needs to be shared with other staff needing the information to provide a customer with effective care and support. So how do we comply with the duty of confidence – yet make sure we provide high quality care?

We implement Confidentiality Measures - which allow information to be shared but only under strict controls to ensure the duty of confidence is maintained. These measures include:

Restricting people - who can have access to the information working on a “need to know basis”

Restricting information - restricting the information that these people can have i.e. providing only the information that is needed for them to do their job, no more and no less, such as staff performing administrative work may need to access customer addresses but not their other personal details.

Training Staff - making sure all employed staff understand their duty of confidence, the confidentiality measures and their responsibilities.

Enforcing - contract clauses, adding confidentiality obligations and disciplinary clauses in employment contracts for all staff and adding confidentiality obligations and penalties in service contracts with external organisations (such as IT Engineers, window cleaners) who might come into contact with information.
These measures are aimed at everyone who might see or overhear confidential information – cleaners, messengers, maintenance staff, IT staff, volunteers, apprentices, caretakers, drivers, etc.

Security Measures

Security Measures protect against risks to the organisation – including risks such as loss, theft or compromise of the information we need to protect. The measures can be grouped into three types:

- Physical measures
- People measures
- Electronic measures

Who should protect information?

The Company Board and the senior management level of the organisation (e.g. a Board) is ultimately responsible for the Company's compliance with all legal obligations – which include the appropriate use and protection of personal information.

When should information be protected?

It should be protected from the time it is created to the time it is destroyed (securely e.g. by shredding or incineration). This means 24 hours a day, 7 days a week wherever the information is located:

- **Locations -** In offices, in briefcases, on trains, in clinics, on wards and whatever format it is in.
- **Formats -** Digital (e.g. e-mail, customer admin systems), hard copy (e.g. customer letters, appointment books, personal notes, health information)

The duty of confidence
The duty of confidentiality remains with all staff even after employment with the Company ends. This is to ensure that information obtained during our employment remains confidential.

INFORMATION TECHNOLOGY

General Advice
In public rooms or rooms to which the public may have access, terminals or screens should be placed facing away from the normal access routes.

Staff should use a password-protected screensaver, lock their workstation or log off if there is someone present who is not authorised to view information or when you leave the computer unsupervised.

Passwords
The use of passwords is the primary method of ensuring data security. There is sometimes a temptation to share passwords or to display them on notes attached to the side of the screen. These and similar practices severely compromise security measures. To ensure that unauthorised access to Company systems is prevented, passwords must be kept private.

Internet Access
The internet link is provided for Company authorised business. Personal use is permitted before or after starting work only with the Line Managers authority and provided this does not interfere with the performance of work duties. A Line Manager can limit personal access to the internet and staff must act in accordance with the guidelines of their Line Manager. The Company takes no direct responsibility for the actions of any individual with regard to the misuse of the internet.

Email
The e-mail system is provided for Company authorised business and the Company takes no direct responsibility for the actions of any individual with regards to misuse of the e-mail system. Due to the insecure nature of internet mail, users must consider e-mail and other information to be public information. Staff should bear in mind that all information produced can be made publicly available under the Freedom of Information Act if it is requested. Staff should not consider information sent or received through the e-mail system as their private information.
Only the following methods are acceptable for emailing customer identifiable information:

- email between users on the same email server'

Note that emails to and from external Companies are NOT secure and should not be used unless suitably encrypted before sending.

Use of Facebook and other Social Media
The employee handbook and code of behaviour make it clear that all employees will not:

- Share confidential information online
- Post comments about colleagues or customers
- Use social networking sites to bully or intimidate colleagues
- Use social networking sites in any way which is unlawful

This list is not intended to be exhaustive. If there is any doubt about whether a particular activity online is acceptable, it can be useful to think through a real-world analogy. For example, manipulated photos that are intended to mock individuals would be considered offensive if printed and pinned on workplace notice boards, and are no less offensive when shared online, even when privately shared between friends. These are disciplinary offences are taken very seriously.

Here are some critical do's and don'ts to remember:

- Don't make disparaging remarks about your Company, its customers or fellow employees on a social network site avoid any identification of your employer on your profile page of a social network site.

- Don't make any remarks on a social network site that may embarrass your employing organisation. In particular, do not air your grievances where countless others might be able to read all about it.

- Don't use the social networking site or other non-work related sites when you are supposed to be working.

- Never post sexually explicit, racially offensive, homophobic or other unlawfully discriminatory remarks on your network site read and comply with your employer's policy on IT use in the workplace.

Social Networking – Assessing the Risks
Any form of online posting can expose you to risk. Message boards and blogs are both considered to be public mediums and material posted on those resources is subject to the same laws as those for print. The best advice is to avoid making comments about your employer and/or work colleagues/management. A few words posted on your blog, Facebook page or message board could be read by numerous people.

Use of Laptops and mobile phones
All laptops, desktops and mobile phones must be password or PIN number protected. They must not be left open for anyone else to access whether working in company premises or at home or other external venues.

Users of laptops and mobile phones must ensure that all sensitive files are password protected (note that these passwords cannot be recovered if lost/forgotten), disks and paper copies containing valuable software or sensitive data must be locked away in briefcases or containers when in transit and particular care should be given to the security of laptops when in transit. They must be securely locked and not left on general view.

Laptops and mobile phones must not contain any customer identifiable information – use an encrypted memory stick and any user taking any equipment home should check that their household insurance covers loss, theft and damage.

Laptops and mobile phones must kept safe at all times. Laptops must not be left out or on their docking bases, they must be left in a locked cupboard or drawer.

Operate a Clear Screen Policy
When you leave your computer you must remember to press “Ctrl" + “Alt" + “Delete" and lock your computer so that it cannot be accessed by anybody who is not authorised. Your computer must only be accessed by using your user name and password and you must not share your password with anyone else.

Operate a Clear C Drive Policy
No data, confidential or not, should be stored on the “C" drive of a computer.

USB/Memory Sticks
Thousands of USB sticks are lost or stolen each year causing personal, sensitive and confidential data to be lost or, more worryingly, exposed. The Information Commissioner, who monitors how we follow the Data Protection Act principles, has been granted the ability to impose higher fines for those who breach any of the rules.

Our Company allows ONLY the use of approved password protected sticks. Speak to your Line Manager if you need one.

What is the Freedom of Information Act?

This Act gives the public a right of access to any files or information held by the Trust. There are some exemptions but the general rule is that we have to provide the information unless we can show there is a good, public interest, reason not to. If a request is turned down, the applicant has a right of appeal to the Information Commissioner, who is appointed by Parliament to ensure that the Act is complied with.

Anybody can make a request under the act – this includes commercial companies, journalists, customers and the public. They have the right to ask for the information they want and there is no need for them to tell us why they want it.

The Act applies to any information held by the Company, in any form – electronic as well as paper records. If your files contain scraps of paper with rough notes you have made or comments, then these are just as disclosable as "official" letters and memos. Emails have to be treated in the same way. You should write everything, including emails, in a way you would not mind them being read by members of the public and the press.

The Act is fully retrospective, which means that it applies to all information, including that created prior to the Act coming into force. It does not apply to requests to see personal data, including health records, which are covered by the Data Protection Act 1998 and the Access to Health Records Act 1990 (if the request is to see the health records of a deceased patient).

Freedom of Information requests have to be made in writing – an email counts as a written request. We have a maximum of 20 working days to confirm whether or not we have the information requested and to provide it.

The Data Protection Act

The Data Protection Act 1998 became law in March 2000. It sets standards which must be satisfied when obtaining, recording, holding, using or disposing of personal data. These are summarised by 8 Data Protection Principles. As well as information held on computers, the Data Protection Act 1998 also covers most manual records e.g.

- Health
- Finance
- Personnel
- Suppliers
- Occupational Health
- Contractors
- Volunteers
- Card Indices

THE 8 DATA PROTECTION PRINCIPLES

Personal data must be:
1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up-to-date
5. Not kept for longer than necessary
6. Processed in accordance with the rights of data subjects
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside the EEA without adequate protection

PRINCIPLE 1 - Processed fairly and lawfully
There should be no surprises, so ... inform data subjects why you are collecting their information, what you are going to do with it and who you may share it with e.g.

- When formulating a research project remember to be open and transparent about what you will be doing with the information
- When working in a team, ensure that the team is aware of who the members of the team are and that all those involved
- Be open, honest and clear

PRINCIPLE 2 - Processed only for specified purposes
Only use personal information for the purpose(s) for which it was obtained e.g.

- Personal information on the Administration System must only be used for employment purposes - not for looking up friends addresses or birthdays
- Only share information outside your team if you are certain it is appropriate and necessary to do so if in doubt, check first!

PRINCIPLE 3 - Adequate, relevant and not excessive
Only collect and keep the information you require. It is not acceptable to hold information unless you have a view as to how it will be used. Do not collect information "just in case it might be useful one day!" e.g.

- Taking both daytime and evening telephone numbers if you know you will only call in the day
- Explain all abbreviations
- Use clear legible writing
- Stick to the facts - avoid personal opinions and comments

PRINCIPLE 4 - Accurate and kept up-to-date
Take care when inputting information to ensure accuracy. How do you know the information is up-to-date? What mechanisms do you have for checking the Information is accurate and up-to-date? e.g.

- Regularly check to confirm that their details are correct - address, telephone number etc.
- Check existing records thoroughly
- Before creating new records
- Avoid creating duplicate records

PRINCIPLE 5 - Not kept for longer than necessary

- Check the Company Records Management Strategy and Guidelines
- Ensure regular housekeeping/spring cleaning of your information
- Do not keep “just in case it might be useful one day!”
- Check the organisation’s disposal policy
- Dispose of your information correctly

PRINCIPLE 6 - Processed in accordance with the rights of data subjects

- Subject access requests
- Confidentiality
- Prevent processing for direct marketing - an end to junk mail and faxes!
- Automated decision taking compensation
- Rectification/blocking/erasure
- Request an assessment

PRINCIPLE 7 - (Practical)
Protected by appropriate security

- Ensure security of confidential faxes by using Safe Haven/Secure faxes
- ALWAYS keep confidential papers locked away
- Do you have a clear desk policy?
- Ensure confidential conversations cannot be overheard
- Keep your password secret
- Ensure information is transported securely

PRINCIPLE 8 - Not transferred outside the European Economic Area (EEA) without adequate protection

- If sending personal information outside the EEA ensure consent is obtained and it is adequately protected
- Be careful about putting personal information on websites - gain consent first
- Check where your information is going e.g.

The EEA comprises: United Kingdom, France, Belgium, Germany, Denmark, Ireland, Netherlands, Sweden, Portugal, Spain, Finland,

To sum up, remember that information must be:

- Held securely and confidentially
- Obtained fairly and efficiently
- Used effectively and ethically
- Recorded accurately and reliably
- Shared appropriately and lawful

In addition your organisation should be protected by appropriate security:

- Good information management practices
- Guidelines on IT security
- Staff training
- Confidentiality clause in employment contracts
- Procedure for access to personal data
- A disposal policy/procedure for confidential information
- Confidentiality contracts with third parties e.g.
    - archiving companies
    - cleaners
    - temporary staff
    - outside contractors

Records Management

We all have a responsibility to ensure that the single largest activity, that of obtaining, storing, disseminating and transferring or destroying information across the Company, complies with Acts/Regulations. All records should be 'CURED':

- **C**reating: Good quality records - are they accurate? Up to date? Easy to find? Free from duplication? Not disjointed?
- **U**sing: Within Acts and Regulations
- **R**etention: Safe storage and archive in line with Company recommended retention schedule
- **E**valuate: Are the records worthy of permanent archive?
- **D**isposal: Appropriately according to policy

Best practice guidance states:

All staff have a legal and professional obligation to be responsible for any records which they create or use in the performance of their duties.

Any record created by an individual, up to the end of its retention period, is a public record and subject to information requests (FOI and DPA)

Law and Guidance – further reading

- Data Protection Act 1998
- Freedom of Information Act 2000
- Information Quality Assurance
- The Human Rights Act 1998 (Article 8)
- The Public Records Act 1958
- Common Law Confidentiality

Local policy and procedure guidelines:

- Data Quality Policy
- Records Management Strategy
- Records Keeping Standards
- Information Management Technology Strategy
- Data Protection Policy
- Freedom of Information Policy
- Information Management Systems Security Policy and Procedures
- Whistle-blowing Policy