Revision History				
Date	Version	Author	Summary of Change	Change made by
15.01.2014	1.0	Chris Scott	New document	N/A
15.01.2015	2.0	Chris Scott	Annual issue	CS
15.01.2016	3.0	Chris Scott	Annual issue	CS
17.03.2016	3.1	Chris Scott	New template	SCW
27.01.2017	3.2	Chris Scott	Update	AS
15.04.2018	4.0	Chris Scott	GDPR Update	AS

Approval			
Date	Version	Approver	Title
15.01.2016	1.0	Phil Miller	Managing director
17.04.2018	4.0	Phil Miller	Managing Director

Principles

In order to operate effectively and fulfil its legal obligations, ABCA Systems needs to collect, maintain and use certain personal information about current, past and prospective employees, customers, suppliers and other individuals with whom it has dealings.

All such personal information, whether held on computer, paper or other media, will be obtained, handled, processed, transported and stored lawfully and correctly, in accordance with the safeguards contained in the General Data Protection Regulations (GDPR).

ABCA Systems is committed to the principles of the GDPR. These principles require that personal information must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Compliance

In order to comply with the GDPR principles, regardless of whether data is stored electronically, on paper or any other material, ABCA Systems will:

- Observe fully all conditions regarding the fair collection and use of personal information;
- Meet its legal obligations to specify the purpose for which information is used;

- Collect and process appropriate personal information only to the extent that it is needed to fulfil operational needs or to comply with legal obligations;
- Ensure the quality of the personal information used;
- Apply strict checks to determine the length of time personal information is held;
- Ensure that individuals about whom information is held are able to exercise their rights under the GDPR, including the right to be informed that processing is taking place, the right of access to their own personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase incorrect information;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred outside the EEA without suitable safeguards.
- User access reviews are carried out every six months to ensure only those who require access are able to access it.

Responsibilities

Overall responsibility for ensuring that ABCA Systems Ltd. complies with its data protection obligations rests with the Managing Director.

The DPO (Data Protection Officer) for ABCA Systems, who will monitor and ensure enforcement of this policy, is Amanda Simmons.

It is the responsibility of all employees to ensure that personal information provided to ABCA Systems Ltd, is accurate and up to date. To this end employees are required to inform ABCA Systems Ltd. immediately when changes occur, for example in relation to home address.

Employees whose role involves the collection, maintenance and processing of personal information about other employees, customers, suppliers or any other individuals with whom ABCA Systems Ltd. Has dealings are responsible for following ABCA Systems Ltd.'s rules on good data protection practice as provided in the GDPR training that is given to all employees and is refreshed six monthly.

The policy also extends to contractors, suppliers and other people working on behalf of ABCA Systems.

Information about employees

ABCA Systems holds the following personal information about its employees which is used for payroll and administrative purposes:

- Name
- Address
- Banking details
- Salary
- Sickness & Absence details

We also hold the following sensitive personal information about employees, which is used for the purpose of equal opportunities monitoring and health and safety monitoring:

- Physical & Mental Health details
- Ethnicity & Nationality information.
- Disciplinary information.

We also, where an employee's role requires, carry out a DBS check and full security screening under the BS7858 regulations. These reports are held in the employee's personnel files and only the appropriate people have access to this file.

General Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- ABCA Systems will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the below guidelines:

    - Compliant passwords (one upper case letter, a special character and eight letter long) are used changed every 90 days.
    - 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.
    - Employees should request help from their line manager or the DPO if they are unsure about any aspect of data protection.
    - Any sharing of personal data that is required should be password protected or encrypted.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to Smart IT or the DPO.

All data is stored via ABCA servers – apart from emails, which are securely stored via office 365, who are fully GDPR compliant.

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

These guidelines also apply to data that is usually stored electronically but has been printed out.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people can see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- Printouts should not be kept for longer than are required for the purposes that it was printed.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Compliant passwords (one upper case letter, a special character and eight letter long) are used changed every 90 days and not shared between employees.
- If data is stored on removable media, this is encrypted so cannot be accessed by anyone else.
- Data should only be stored on designated drivers and servers and should only be uploaded to an approved cloud computing services
- Data is backed up frequently, these backups are tested regularly.
- Data is not to be saved directly to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data are protected by approved security software and a firewall.
- Mobile laptops/phones are protected by encryption software, to protect the data if these devices are lost or stolen.
- Backups between the Oldham and Newcastle servers are encrypted so data is secure when it is backed up.

Data Accuracy

The law requires ABCA Systems to take reasonable steps to ensure data is kept accurate and up to date. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept up to date as possible.

- 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, for example, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Access to information

Anyone who is the subject of personal information held by ABCA Systems Ltd. has the right to make a Subject Access Request (SAR). Employees who wish to exercise this right should write to the HR Manager.

All individuals who are the subject of personal data held by ABCA systems are entitled to:

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

If, as the result of a SAR, any personal information is found to be incorrect, it will be amended.

ABCA Systems Ltd. will deal promptly with SAR's and will normally respond within 30 days. If there is a reason for delay, the person making the request will be informed accordingly.

The data controller will always verify the identity of anyone making a subject access request before handing over information.

Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances ABCA Systems will disclose requested data. However, the DPO will ensure the request is legitimate.

IT communications and monitoring

ABCA Systems provides employees with access to various computer facilities for work and communication purposes. In order to ensure compliance with all applicable laws in relation to data protection, information security and compliance monitoring, ABCA Systems Ltd. has adopted a Technology Security Policy, which should be read in conjunction with this Data Protection Policy.

Retention and Destruction Times

Personal data of an employee, customer, supplier or subcontractor will only be held on file until it is no longer needed, unless it may be required for historical, statistical or research purposes. However, it must be deleted once it is no longer required for these purposes. Data stored electronically will be deleted from the network drives, but still held on the server for 2 weeks after deletion. It will then be permanently deleted.

Breach of the policy

Breach of this policy will be regarded as a disciplinary offence and will be dealt with under ABCA System's Ltd.'s formal discipline procedure.

Employees who consider that there has been a breach of this policy in relation to personal information about them held by the ABCA Systems Ltd. should raise the matter via the formal grievance procedure.

If an employee suspects a data breach, or knowingly has caused a breach they should report this to their line manager immediately, who will report it to the company DPO, who can report the breach to ICO within 72 hours of the breach occurring.

Data Incidents

A data incident is where confidential, protected or sensitive information is either lost, misused, amended or disclosed to a person who should not have access to it.

Examples

- If you have added inaccurate contact information to a customer's account (e.g. wrong contact number, address, email address)
- If you have accidentally disclosed any customer information to the wrong customer such as address, contact details, or anything that could identify the customer in some way
- If you receive a call or email from a customer, non-customer or third party who suspects data may have been lost, altered, misused or disclosed in error.
- If you have had any company device stolen, such as a laptop, phone, PDA or external hard drive

Everyone needs to know how to report a suspected data incident. Unfortunately, mistakes can happen, so it's equally important that we all know how to spot a data incident. Not all incidents are breaches, but we still need to know about them.

If you suspect a data incident has occurred then it must be reported to the DPO, HR and your Department Head as soon as you become aware of them – even if you're not sure it's a data incident or you don't have all the information. Some data incidents must be notified to the ICO within 24 hours therefore it is important you report a suspected data incident immediately.

If you are reporting a data incident, then title your email 'Potential Data Incident' and include the following info:

- Your name and contact information
- How, when and where did the incident occur.