Data Breach and Complaints Reporting Procedure



Revision History				
Date	Version	Author	Summary of Change	Change made by
15.01.2016	1.0	Chris Scott	New document	CS
17.03.2016	1.1	Chris Scott	New template	SCW

Approval			
Date	Version	Approver	Title
15.01.2016	1.0	Phil Miller	Managing director

Introduction

ABCA holds and processes data relating to:

- Customers
- Employees
- Suppliers

As such, we have a legal obligation to protect that data and under the Data Protection Act, we must:

- Only collect data that we need for a specific purpose
- Always keep that data secure
- Ensure that the data is relevant and secure
- Only hold as much data as we need and not keep for a longer time than it is required
- Allow the customer / employee / supplier to see that information on request

If a person or company who we hold data on believes that it has been misused or that we haven't kept it secure, then the first step is for that person or company to contact us and advise us.

We should handle that request according to the procedures outlined in this document. If the person or company who we hold data on is unhappy with our response, then they should contact the Information Commissioner's Office (ICO).

What could be classed as a Data Complaint?

- Unwanted contact attempts
- Customers could deem out contact attempts as nuisance calls
- A nuisance call is an unwanted telephone call, email or text
- Inability to access information we hold
- Customers should be able to access any information we hold about them
- Re-use of information we hold
- Customers information held by us should not be re-used for a purpose other than which it was obtained in the first place
- We have mishandled information
- A customer may make a complaint about how we handle the information we have (e.g. it is wrong or we have disclosed it to a 3rd party)

What information is an individual entitled to?

A request made by someone who wants to see a copy of the data we hold about them is called a Subject Access Request (SAR), and their right to see the data we hold is conveyed on them by the Data Protection Act.

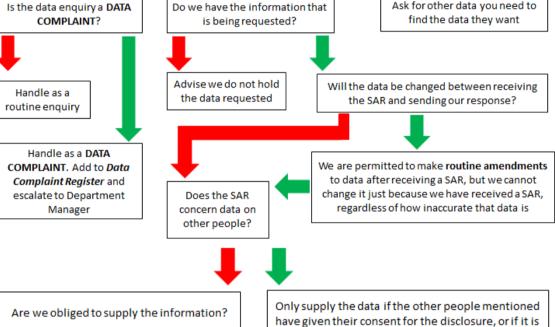
We should act promptly to deal with a SAR and should respond no later than 40 calendar days following receipt of the SAR.

How should you handle a request for information?

All staff are required to have completed Data Protection Training and be able to identify a SAR. The following flow chart should allow you to handle any request for information, be it a SAR, Data Complaint or Data Enquiry.

ASLGN134	Page 1 of 2	V1.1 0316 CS	APPROVED: PM
----------	-------------	--------------	--------------

Ultimately, you should ensure that any Data Breaches or Data Complaints are recorded on the relevant register, and the request is escalated to a Department Manager as soon as is practicable. The following flow chart is provided as a decision-making tool to be used in receipt of a data request. Where the answer to the question is Yes, follow the green arrow Where the answer to the question is No, follow the red arrow Handle as a SAR. Add to the Data Breach Register and escalate to Branch Manager. Do Is the request a formal Ask for evidence you have enough data to confirm the identity SUBJECT ACCESS REQUEST? of their identity of the individual making the SAR? Do you need more data to find Advise the individual that we do Handle as a DATA ENQUIRY out what they want? not charge a fee for a SAR Ask for other data you need to Is the data enquiry a DATA Do we have the information that COMPLAINT? find the data they want is being requested?



deemed reasonable to supply that information without the other person's consent. If it is decided that other people's data should not be disclosed, then we should still disclose as much information as possible by redacting references to the other person

exempt from SAR, then our response should be that we do not hold any of their personal data that we are required to reveal Prepare the response by removing complex terms, and provide a copy of the data requested in a permanent written form by post, unless the individual agrees otherwise, or doing so would be impossible to it would involve disproportionate effort (in which consideration should be given to providing the data in a permanent and secure

If the data requested is

Employee Signature	Employer signature	
Date	Date	

electronic format

ASLGN134 Page 2 of 2	V1.1 0316 CS	APPROVED: PM
----------------------	--------------	--------------