Wealth Wizards

## Introduction

This is the policy of the 'Wealth Wizards Group', which is Wealth Wizards Limited and its subsidiaries from time to time including Wealth Wizards Advisers Limited and Wealth Wizards Benefits Limited.

# The Legislation

## Data Protection Act 1998 (DPA 1998)

Data protection obligations are currently set out in the Data Protection Act 1998 (DPA 1998). The DPA 1998 implements the EU Data Protection Directive (95/46/EEC), which introduced an extensive data protection regime by imposing broad obligations on those who collect personal data and by conferring broad rights on individuals about whom data is collected. The DPA 1998 sets out when personal data can lawfully be processed and how it should be processed. It governs processing by data controllers of personal data relating to data subjects.

The DPA 1998 will be repealed by the Data Protection Bill.

## Reform of the law at EU level: GDPR

In April 2016, the European Parliament approved a general data protection reform package, thereby bringing to a close nearly four years of work overhauling the EU's data protection rules.

## Data Protection Bill (DPB)

In June 2017, the government announced that the DPA 1998 would be replaced by a new Data Protection Bill (DPB). It is intended that the DPB, supplemented by the **GDPR**, will modernise data protection law in the UK given the demands of an increasingly digital economy and society. When the UK leaves the EU, the **GDPR** will be incorporated into UK domestic law under the European Union (Withdrawal) Bill currently before Parliament.

The four main areas covered by the DPB are:

- General data processing (which will be relevant to an **employer's** day-to-day dealings with its workforce).
- Law enforcement data processing (the DPB will implement the DPLED).
- Data processing for national security purposes (including processing by the intelligence services).
- Regulatory oversight and enforcement by the Information Commissioner's Office (ICO).

Wealth Wizards Limited is a data processor. Wealth Wizards Advisers Limited and Wealth Wizards Benefits Limited are data controllers and are registered with the Information Commissioner's Office.

### The Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) is an independent public body responsible for upholding information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The **GDPR** requires every member state to provide one or more independent public authorities to be responsible, as a "supervisory authority", for monitoring its application, in order to protect the fundamental rights of individuals in relation to processing and to facilitate the free flow of personal data within the EU (*Article 51(1)*). The DPB confirms that the ICO will continue and will be the supervisory authority in the UK (*clauses 112(1) and 113(1)*).

Data controllers, and (where applicable) their representatives must co-operate on request with the ICO in the performance of its tasks (*Article 31*, ***GDPR***).

#### The GDPR and DPB: concepts and definitions

The **GDPR** and DPB together create a new regime which will govern the processing by data controllers of personal data relating to data subjects. As it is put in recital 11 to the **GDPR**:

"Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States."

Under the new regime, the definition of personal data is more detailed and reflects changes in technology and the means organisations use to collect information about people. Data controllers, will still be required to comply with a set of principles for processing personal data. The new principle of accountability requires data controllers to show how they have complied with the principles. For example, data controllers will not only need to have policies which demonstrate that they comply with the principles but they will also need to be able to show how the policies have been implemented.

# Definitions

**Data Subject** - the identified or identifiable living individual to whom personal data relates .

**Personal data** - data held or likely to be held about a living individual who can be identified from the data, including any expression of opinion about the individual. Personal data includes;

- CCTV footage if it could be used to match an image to a photo, description or physical image of an individual.
- An identifier such as a name, an identification number, location data or an online identifier.
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- Web based tracking technology used with the intention of linking the web user to a name and address would also be considered personal data.

The GDPR does not apply to the personal data of the deceased.

**Special categories of personal data (currently sensitive personal data)** - Under the DPB, read with the GDPR, there are slight changes to the categories of sensitive personal data currently identified by the DPA

1998 and which are now identified as “special categories of personal data” (*Article 9(1), GDPR*). This includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health, sex life and sexual orientation.

Processing of the special categories of personal data is prohibited unless an exception applies (*Article 9(2), **GDPR***).

The commission or alleged commission of any offence and criminal proceedings are no longer included in the special categories of personal data. They are dealt with separately under the new regime, Criminal convictions and offences.

**Data Controller** - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU law or member state law, the controller or the specific criteria for its nomination may be provided for by EU law or member state law (*clause 5(1), DPB and Article 4(7), **GDPR***).

**Data Processor** - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (*Article 4(8), **GDPR***).

**Pseudonymisation** - the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person (*Article 4(5), **GDPR***).

Recital 28 of the **GDPR** recognises that applying pseudonymisation to personal data can reduce the risks to the data subjects concerned and enable data controllers to meet their obligations. Pseudonymised personal data can still be covered by the **GDPR** if, with additional information, the personal data can be attributed to a particular person.

It should be possible for a controller to use pseudonymisation in internal processes, as long as care is taken to identify those authorised to process the data and as long as the additional information needed to attribute the personal data to a specific data subject is kept separate (*recital 29, **GDPR***).

**Anonymisation - t**here is a distinction between information that has been pseudonymised and information that is anonymous. The **GDPR** does not apply to anonymous information, namely information which does not relate to an identified or identifiable person, or to personal data which has been anonymised so that the data subject is not, or is no longer, identifiable (*recital 26, **GDPR***). This means that the processing of anonymous information for statistical or research purposes is not covered by the **GDPR**.

The ICO produced Anonymisation: managing data protection risk code of practice, which provides guidance on the way in which data can be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.

**Processing personal data** - The processing of personal data means an operation (or set of operations) which is performed on personal data (or on sets of personal data), such as:

- Collection, recording, organisation, structuring or storage.
- Adaption or alteration.
- Retrieval, consultation or use.

- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Restriction, destruction or erasure.

Processing of personal data must be carried out in accordance with the data protection principles.

**Automated decision-making (including profiling)** - Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal, or similarly significant, effects. Recital 71 of the **GDPR** gives e-recruiting practices which have no human intervention as an example of automated processing. There are limited exceptions to this right which are considered below.

The circumstances in which data subjects can be subject to a decision based solely on automated decision-making, including profiling, are those in which the decision is:

- Necessary for entering into, or performance of, a contract between the data subject and a controller.
- Based on the data subject's explicit consent.
- Authorised by EU law or member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

In the first two of the exceptions, the data controller must implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, being at least the right to:

- Obtain human intervention.
- Express their point of view.
- Contest the decision.

Decisions may not be based on the special categories of personal data unless either the data subject has given explicit consent or the processing is necessary for reasons of substantial public interest and, in either case, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests have been put in place.

**Profiling** - Profiling is any automated processing of personal data which evaluates an individual in order to analyse or predict such things as their performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

Recital 71 of the **GDPR** suggests that in order to ensure fair and transparent processing, taking into account the specific circumstances and context in which the personal data is processed, the controller should:

- Use appropriate mathematical or statistical procedures for the profiling.
- Implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised.
- Secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.

**Processing personal data in the context of employment** - Under the **GDPR**, it is open to member states to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for:

- The purposes of recruitment.
- The performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements.
- The management, planning and organisation of work.
- Equality and diversity in the workplace.
- Health and safety at work.
- Protection of the **employer's** or customers' property.
- For the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment.
- For the purpose of the termination of the employment relationship.

Any such rules must include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to:

- The transparency of processing.
- The transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

The DPB makes specific provision for the processing of special categories of personal data when it is necessary for the carrying out of rights or obligations under employment law.

# Data protection principles

The **GDPR** sets out a number of principles with which data controllers must comply when processing personal data (*Article 5*).

| | |
|---|---|
| **Lawfulness, fairness and transparency** | Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject |
| **Purpose limitation** | Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose |
| **Data minimalisation** | Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed |
| **Accuracy** | Personal data shall be accurate and, where necessary, kept up to date |
| **Storage limitation** | Personal data shall be 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 |
| **Integrity and confidentiality** | Personal data shall be 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 |
| **Accountability** | The controller shall be responsible for, and be able to demonstrate compliance with the GDPR |

## Conditions for lawful processing under Article 6(1)

Processing personal data will be lawful only if, and to the extent that, at least one of the conditions in Article 6 of the **GDPR** is met. Those conditions (which are similar those under the DPA 1998) are that:

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of a data subject prior to entering into a contract
- The processing is necessary to comply with a legal obligation to which the controller is subject
- The processing is necessary to protect the vital interests of the data subject or another person
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests and fundamental rights and freedoms of the data subject which require protection of personal data, especially were the data subject is a child

## Criminal Offence Data

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of official authority. Article 10 says:

*"Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."*

This means you must either be processing the data in an official capacity, or have specific legal authorisation – which in the UK, is likely to mean a condition under the Data Protection Bill and compliance with the additional safeguards set out in the Bill. We will publish more detailed guidance on the conditions in the Bill once these provisions are finalised.

Even if you have a condition for processing offence data, you can only keep a comprehensive register of criminal convictions if you are doing so in an official capacity.

Wealth Wizards

# Data Controller Requirements and Duties

## Notifying the Information Commissioner

The Data Protection Act 1998 requires **data controllers** to give details about their processing of personal information to the Information Commissioner for inclusion in a public register, unless they are exempt.

The registration must be renewed annually.

The Data Protection registration number for Wealth Wizards Advisers Limited is: Z2323485. The Data Protection registration number for Wealth Wizards Benefits Limited is: ZA163085.

### Notification process

The details to be notified are:

- name and address of the data controller or their representative
- description of the information being processed
- purpose of processing the information
- those to whom the information will be or may be disclosed
- countries outside the European Economic Area (the EU plus Norway, Iceland and Liechtenstein) where data may be transferred
- certain details on information security measures

Notification can be initiated by calling the Information Commissioner Notification Line on Telephone: 01625 545 740, or by completing and posting a notification form, which can be obtained from https://forms.informationcommissioner.gov.uk/cgi-bin/dprproc?page=7.html

The period of notification is one year. Notifications must be renewed annually. There is an annual fee of £35. Changes to a notification entry must be notified as soon as possible and are made free of charge.

Wealth Wizards Advisers Limited and Wealth Wizards Benefits Limited are the Data controllers and responsible for all the data held on their clients. The DPC for Wealth Wizards Advisers and Wealth Wizards Benefits Limited is the Governance & Information Security Manager.

## Bogus agencies

Businesses throughout the UK continue to be troubled by bogus data protection notification agencies. The Information Commissioner is the only statutory authority for administering and maintaining the public register of data controllers.

# Right of Access (Subject Access Requests)

In general terms customers have a right of access to personal information, the purpose for which the information is being held and whom the information is being disclosed to.

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- We have one month to respond to a request.
- We cannot charge a fee to deal with a request in most circumstances.

Wealth Wizards

## Enforcement and penalties

### When to inform the ICO of a data breach

Under the current Data Protection Act the ICO expects to be informed about serious breaches of data protection. This is to change under the GDPR. A breach notification will be mandatory and any personal data breach must be notified to the ICO within **72 hours of awareness** and to the individual affected "without undue delay".

As a result, organisations will be required to amend their internal processes relating to the handling of data breaches to ensure that the notification requirement is complied with.

## ICO Investigative Powers

Upon receipt of a notification or information concerning a data breach under the GDPR, the ICO is provided with increased powers of investigation including:

- ordering the controller and the processor to provide information necessary to perform its tasks;
- carrying out a data protection audit;
- reviewing certificates;
- notifying the controller or processor of any alleged infringement of the GDPR;
- obtaining from controller or processor access to all personal data and all information necessary to perform its tasks; and
- obtaining access to any premises of controller and processor including data processing equipment.

## ICO Corrective powers

The ICO may also take corrective measures when investigating a data breach. Some of the corrective powers that can be imposed by the ICO could have a considerable impact on the day-to-day running of a business. Such corrective measures include:

- Issuing warnings to a controller or processor that intended processing operations are likely to result in infringement of the GDPR.
- Issuing reprimands to a controller or processor where processing operations have infringed provisions of the GDPR.
- Ordering the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the GDPR.
- Ordering the controller or processor to bring processing operations into compliance with the GDPR.
- Ordering the controller to communicate a personal data breach to the data subject.
- Imposing a temporary or definitive limitation including a ban on processing.
- Ordering the rectification, restriction or erasure of personal data.
- Withdrawing a certification or ordering a certification body not to issue a certificate.
- Imposing administrative fines.
- Ordering the suspension of data flows to a recipient in a third country or to an international organisation.

### ICO Enforcement powers

In addition to control measures, the GDPR also provides the ICO with stronger enforcement powers and powers to impose higher monetary penalties. The ICO will have the power to issue hefty fines of up to €20 million (approximately £17 million) or up to 4% of an organisation's annual global turnover. The GDPR splits the fines into two groups.

1) The organisation will be subject to the maximum fine of up to **€20 million**, or up to 4% of the organisation's global annual turnover, whichever is higher, where the following provisions have been infringed:

- the basic principles for processing data (including conditions of consent);
- the data subject's rights;
- the transfers of personal data to a recipient in a third county or an international organisation;
- any obligations pursuant to adopted member state law; and
- non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows.

2) The organisation will be subject to the maximum fine of up to **€10 million**, or up to 2% of an organisation's global annual turnover, whichever is higher, if an organisation infringes the requisite provisions relating to the obligations of: the controller and the processor, the certification body, or the monitoring body.

The obvious concern is that such high fines may have a serious impact on the health of a business. However, whilst each fine is to be “effective, proportionate and dissuasive”, the facts of each individual case will be taken into account as will mitigating factors such as the nature, gravity and duration of the breach, timing of the notification to the ICO, degree of co-operation from the organisation with the ICO and compliance with corrective measures.

# Client Data

It is vital that we take the protection of our clients' personal data with the utmost of seriousness.

Appropriate systems and controls need to be in place to ensure the secure storage of personal data. In addition, process and procedures need to be in place and training and awareness given to all staff who handle client data in their day to day roles. The following section of this document is designed to provide company policy on processing and storing client data for all back-office staff.

### How data loss occurs

Due to the nature of our business we have to hold lots of data about our clients; most of it very sensitive and personal. Despite the data protection act’s requirements for firms to ensure that any client data they hold is secure data is sometimes lost, either through error - for example if an employee loses a company laptop - or theft.

The most common reason for loss of data at present is theft of a portable device such as a laptop or memory stick.

## How lost data is used for identity fraud

The implications of data loss can be very serious. Criminals who get hold of personal sensitive information such as national insurance numbers and banking details can use that information to commit identify fraud. On the whole, these types of crimes are carried out by organised groups but sometimes can be the work of the opportunistic criminal but either way the impact on the client can be extremely serious. Victims of identify fraud are not only severely inconvenienced but their credit records can be damaged and a huge amount of time and effort is often needed to repair the damage left by the fraudster.

The secure handling of client data is not only a requirement under the Data Protection Act but is also a part of the FCA Treating Customers Fairly principle which all firms must adhere to. It is the responsibility of each and every one of us that if and when we have access to sensitive and personal client data that we ensure it is used, stored and transported securely.

## Fair Processing Notification statement

Before we take any personal information from clients we must provide them with a Fair Processing Notification statement explaining how information about them will be treated by us. This is included in the Terms of Business.

Our website also includes a Data Protection Act statement (Privacy Policy).

The client should also be given the opportunity not to receive information in the future from us.

## Telephone requests for information:

From clients

A security check must be completed before any information is given either to a customer or another adviser/provider in order that their identity may be confirmed.

A customer requesting information must be asked to confirm at least 2 of the following:

- National Insurance number
- Full address and postcode
- Date of birth
- Maiden name (if applicable)

It is NOT acceptable to identify a client purely on the adviser or member of staff recognising a client's voice. In all circumstances, even if you feel you know the client you should always ask 2 security questions for certainty. Although it may seem far-fetched this could present significant opportunities for identity fraudsters by impersonating a client and obtaining information to commit identity fraud.

Information requests from a spouse or relative (telephone)

A request for information by the spouse or relative of a client, irrespective of whether or not they are also our client, must not be disclosed via email or over the telephone to the spouse or relative without the client's up to date written consent. If written consent has not been provided, then the information requested should be posted directly to the client.

From a third party

If a third party (product provider, other adviser, etc.) requests information about a customer, then the following checks must be undertaken:

Obtain authority to release information to the third party as follows:

| **Third Party requesting information** | Evidence of authority |
|---|---|
| **Product provider** | The customer must either have an existing or proposed application with the provider. The 3rd party product provider should have a policy number or confirm some details of the policy they are calling about. If in doubt send the information direct to the client. |
| **Another adviser, including the client's accountant/solicitor** | Written letter of authority from the client (see appendix II) |
| **Enduring Power of Attorney** | Certified copy of the enduring power of attorney document. The certification should be a person such as a lawyer or bank official. |
| **Trustees** | Certified copy of the trust deed - as above |

## Email requests for information:

### From clients

It is imperative that an additional security check is completed when receiving emails from clients requesting changes to key identification information, specifically change of address, change of name or change of bank details. This procedure also applies to a request to facilitate an encashment.

In all cases, the client should be phoned and asked to confirm their instructions relating to the email. Once confirmed, a file note should be maintained and the necessary action taken.

It is NOT acceptable to act solely upon the email for these key areas as this could present significant opportunities for fraudsters and scammers.

In the unlikely situation where we cannot conduct the above or we do not have a phone number for the client, please refer to Compliance for further guidance.

Information requests from a spouse or relative A request for information by the spouse or relative of a client, irrespective of whether they are also our client, must not be disclosed via email to the spouse or relative, without verification from the client and the client's up to date written consent ie a letter. If written consent has not been provided then the information requested should be posted to the client.

### From a third party

If a third party (product provider, other adviser etc.) requests information about a customer via email, a phone call to the third party should be made asking them to confirm their instructions. In addition, the checks listed under Telephone Requests From a Third Party in the DPA procedures MUST be undertaken.

## Security of data

### Paper records

Although the majority of client data will be held electronically and covered under the IT security information policy, there are still paper client files that exist and that are still used around the various office locations.

All paper files should be kept in the relevant office that relates to that client and the adviser/firm servicing that client. A paper file should only be taken offsite if the secure transportation and storage is being used.

Wealth Wizards operates a clear desk policy. What this means is that all personal and sensitive client information must be locked away when not in use and not left lying around on desks.

Any client information that has been copied from the client file and no longer required should be shredded – a shredder is available in the office.

## Dos and Don'ts

### DO

- Lock away files when not in use
- Keep all client files in the office
- Operate a clear desk policy
- Place all unwanted client information in the confidential waste or shred

### DON'T

- Leave client files lying around when not in use
- Remove files from the office unless secure transport and storage is being used
- Put confidential client information in the normal waste bin

## What is classed as confidential waste?

Confidential waste is anything that contains details of business or personal nature such as medical history, test results, bank details anything that is potentially damaging to others if it got into the wrong hands. If you are in doubt whether the waste you have is confidential or not shred it anyway to be on the safe side, never put it in the normal waste if you are not sure.

## Collecting and Updating Client data

Client data should only be collected if it is relevant to the information required for a particular business purpose. Client permission should be asked before gathering the data and an explanation given as to why it is needed. Should any of the client's data change this should be updated as soon as possible. If there is

any personal data, we hold that is no longer required and we are not required to keep the data for FCA purposes this should be deleted or destroyed securely.

Anyone who releases client records without authority and consent will be committing an offence.

## Computer Data

Only authorised personnel should have access to client records, access can only be granted via a secure user ID and strong password which can only be authorised by IT.

**All Wealth Wizards computers have a user ID and password to be able to log onto the network. It is vital that you keep that password to yourself and DO NOT allow anyone to log on using your ID and password.**

**You must choose a memorable password for your work account(s) that is not easily guessable and contains a combination of at least 10 letters, numbers and special characters. This should be different to any that you use for personal accounts.**

Whenever you leave your desk ensure that the screen it locked by pressing - ctrl - alt and delete and selecting lock screen

From the same screen, you can also change your password. As there is always the risk that someone may guess your password so try to use a password other than the name of a relative, pets' names or your favourite football team. Your password will automatically require changing, as required by WW rules.

Your computer screen should be positioned so that it cannot be overlooked by non-authorised personnel or other clients.

## Dos and Don'ts

### DO

- Lock your screen when away from your desk
- Change your password regularly
- Position your screen so non-authorised personnel can't see it

### DON'T

- Leave your desk with client data on your screen without locking it
- Give your password to anyone else to use
- Use passwords that people could easily guess
- Refer to the IT data security policy for full details on computer data and storage.

## Telephone Calls

Telephone calls to clients that may involve discussing personal information should not be made in places where non-authorised personnel or other customers may overhear the call. Make sure you are either in an area with authorised personnel or move to a secure area before making any client calls.

## Ex-advisers and client contact

Any adviser who contacts clients that do not belong to them after they have left our service will be in breach of DPA as it is us and not the adviser who is licensed to handle client information. For example, if

an adviser has his own client bank which he takes with him when he leaves then he is OK to contact these, if however, those clients belong to Wealth Wizards for example and the adviser leaves he is not able to contact those clients as he will no longer be authorised to do so under the data protection. Advisers who have their own DP licence will not be in breach of DPA if they contact clients, however this may be prohibited under their adviser agreement.

Any complaints received by us from clients who have been contacted by an ex-adviser against their wishes should be referred to Compliance in the first instance; they may then refer the complaint to the Data Commissioner's office for further investigation.

## IT Data Storage

**The IT information security policy contains full and detailed policies and procedures relating to IT and security. The following paragraph just gives a brief outline of some Dos & Don'ts relating to this area.**

It is company policy that client data should only be stored via a secure network which has a user ID and strong password. WW use Intelligent Office as their client management system.

Hard drives on desk tops and laptops should not be used to store client sensitive data as hard drives can easily be removed and used on another machine without password protection and the data easily removed and potentially used in identity fraud.

All laptops should be taken home and transported and stored securely.

The use of a memory stick or any other portable storage device is prohibited.

Client personal data under no circumstances should be transferred to a CD and posted out to advisers using the normal Royal Mail postal service. Any documents or information that does need to be transported should do so via a secure method such as a courier at the expense of the adviser requesting the information.

## Dos and Don'ts

### DO

- Store client data via a password protected network (IO / Sharepoint)
- Take all laptops home and transport securely

### DON'T

- Do not store client data on the hard drive of a laptop or desk top.
- Leave laptops unsecure when not in use.
- Send client data on CD or any other media via the royal mail normal postal service.

## Data Security breaches

In the event that any data security issues, incidents or breaches occur then the Information Security Incident Handling Procedure must be followed.

Wealth Wizards has an open door policy and encourages all staff to report any data security issues as soon as they become aware of them. The sooner the problem is reported the sooner the risk can be assessed and the problem resolved with minimum impact. Controls can then be put in place to control the weakness and future data losses. In some circumstances when client data is lost it may be appropriate to contact the

client and inform them of the situation.  Clients have a right to know what has happened to their personal information so they can take steps to protect themselves from identify fraud. The decision whether to contact the client will be made by the Chief Executive once the risk assessment has taken place.

# Staff Training

All staff will be made aware of how to process and store customer information confidentially and accurately, and to ensure it is seen by nobody that is not authorised to see that information.

Training will be provided at induction in respect of the following, where appropriate to the role:

- Inputting data onto the computer
- Dealing with telephone enquiries and required security questions
- Security of paper and computer records
- Archiving customer information.

Staff will then complete a Knowledge Test to assess their understanding of the process.

An annual test will be given undertaken by all staff to ensure knowledge is kept up to date, and any changes in the Data Protection Act will be cascaded as they arise.

# Staff Check List

Keeping Personal Information Secure

## Reminder of what you should be doing:

- To keep passwords secure – change regularly, do not share, use passwords that will not be easily guessed by others
- Remember you are responsible for all computer transactions that are made with your own user ID and password
- Lock / log off computers when you are away from your desk
- To dispose of confidential paper waste securely by placing in shredding bins
- To prevent virus attacks by taking care when opening email and attachments or visiting new websites
- Working on a 'clear desk' basis – by securely storing hard copy personal information when it is not being used
- Position computer screens away from windows to prevent accidental disclosure of personal information
- To securely transport and protect personal / sensitive information that is being taken out of the office if it would cause damage or distress if lost or stolen
- Not to take shared portable equipment such as laptop computers out of company premises without the informed consent of their line manager
- Exercise care to safeguard the valuable electronic equipment assigned to them as if they neglect this duty they may be accountable for any loss or damage that may result
- Not to store personal client information on the hard drive of any computer.

## Disclosing customer personal information over the telephone

What you need to be aware of:

- Be aware that there are people who may try to trick you into giving out personal information
- To prevent this from happening you should carry out identity checks before giving out personal information to someone making an incoming call i.e. ask security questions.
- To perform similar checks when making outgoing calls - to ensure you are speaking to the right person
- Limit the amount of personal information given out over the telephone and then to follow up with written confirmation if necessary
- If in any doubt don't give any verbal information and send the information request in writing to the client's home address.

## Notifying under the Data Protection Act

You will need to be aware that:

- We have a notification entry with the Information Commissioners Office (ICO)
- We need to monitor changes in business use of personal information, and notify the ICO if appropriate

## Handling requests from individuals to access their own information

You need to be aware:

- That people have a right to have a copy of the personal information we hold about them
- Of what a subject access request looks like
- Who to pass it to if it is not your responsibility to answer
- That as a company we have a maximum of 1 month days to respond
- That you may need to check the identity of the requester
- What to do if other people's information is contained in the proposed response