

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

### Key Details

<b>Policy Prepared by</b>	Elizabeth Endzweig
<b>Approved by Board / Management in</b>	Elizabeth Endzweig
<b>Policy became operational on</b>	01/05/2018
<b>Next Review Date</b>	01/05/2019

### Introduction

Midos Management Co Ltd are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data information about individuals in order to carry on our work.

These individuals can include customers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This personal information must be collected and dealt with appropriately.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union which will replace the existing 1995 Data Protection Directive (Directive 95/46/EC) from 25<sup>th</sup> May 2018.

Personal data that is collected by the Organisation can be held on computers, laptops and mobile devices, or in a manual file, and includes, but not limited to; email, addresses; passport details; bank details; NI numbers.

The Midos Management Co Ltd will remain the data controller for the information held. The management and staff will be personally responsible for processing and using personal information in accordance with the Data Protection Act and as such will have Data Processor requirements as part of their working requirements.

All management and staff, who have access to personal information, will be expected to read and comply with this policy.

### Purpose

The purpose of this policy is to set out the Midos Management Co Ltd commitment and procedures for protecting personal data. The service regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

This data protection policy ensures Midos Management Co Ltd:

- Complies with Data Protection Law and follows best practice
- Protects the rights of staff, customers and partners
- Is open and transparent about how it stores and processes individuals' data
- Protects itself from the risks of data breach

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

## The Data Protection Law

The Data Protection Act 1998 describes how organisations – including Midos Management Co Ltd – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles, which say “Personal data”:

1. Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s),
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary,
6. Shall be processed in accordance with the rights of data subjects under the Act,
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The following list contains definitions of the technical terms we have used and is intended to aid understanding of this policy:

**Data Controller** – The person who (either alone or with others) decides what personal information Midos Management Co Ltd will hold and how it will be held or used.

**Data Protection Act 1998** – The UK legislation that provides a framework for responsible behaviour by those using personal information.

**Data Protection Officer** – The person of the management who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998.

**Data Subject** – The individual whose personal information is being held or processed by SERVICE NAME (for example: a service user or a staff member)

**‘Explicit’ consent** – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.

Explicit consent is needed for processing sensitive data this includes the following:

- (a) racial or ethnic origin of the data subject
- (b) political opinions
- (c) religious beliefs or other beliefs of a similar nature

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

- (d) trade union membership
- (e) physical or mental health or condition
- (f) sexual orientation
- (g) criminal record
- (h) proceedings for any offence committed or alleged to have been committed

**Notification** – Notifying the Information Commissioners Office (ICO) about the data processing activities of the Midos Management Co Ltd.

**Information Commissioner** – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

**Processing** – means collecting, amending, handling, storing or disclosing personal information.

**Personal Information** – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual users of service and/or employees.

#### **Applying the Data Protection Act within our service**

Whilst access to personal information is limited to management and staff we regularly undertake tasks which involve the collection of personal details including:

- from users of our services
- employees in recruitment

In such circumstances, we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

#### **Data Protection Risks**

This policy helps to protect Midos Management Co Ltd from some very real data security risks, including:

- Breaches of confidentiality: for example, information being given out inappropriately
- Failing to offer choice: for example, all individuals should be free to choose how the organisation uses data relating to them
- Reputational damage: for example, the organisation could suffer if hackers successfully gained access to sensitive data

Security breaches must now be reported within 72 hours of discovery. If we discover a breach that could threaten the data security of customers, we will now inform them of what has potentially been stolen and what that means for them within 72 hours.

**Please see Appendices for Breach Notification Procedure**

#### **Responsibilities**

The Midos Management Co Ltd is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

The management will take into account legal requirements and ensure that it is properly implemented, and will through appropriate management, strict application of criteria and controls:

- a) Observe fully conditions regarding the fair collection and use of information.
- b) Meet its legal obligations to specify the purposes for which information is used.
- c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
- d) Ensure the quality of information used.
- e) Ensure that the rights of people about whom information is held, can be fully exercised under the Act.

These include:

- i. The right to be informed that processing is being undertaken
  - ii. The right of access to one's personal information
  - iii. The right to prevent processing in certain circumstances, and
  - iv. The right to correct, rectify, block or erase information which is regarded as wrong information
- f) Take appropriate technical and organisational security measures to safeguard personal information,
- g) Ensure that personal information is not transferred abroad without suitable safeguards,
- h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- i) Set out clear procedures for responding to requests for information.

**The Data Protection Officer on the organisation is:**

**Name: Elizabeth Endzweig**  
**Contact Details: 0208 800 3366**

**The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:**

- a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- b) Everyone processing personal information is appropriately trained to do so
- c) Everyone processing personal information is appropriately supervised
- d) Anybody wanting to make enquiries about handling personal information knows what to do
- e) Dealing promptly and courteously with any enquiries about handling personal information
- f) Describe clearly how the service handles personal information
- g) Will regularly review and audit the ways it holds, manages and uses personal information
- h) Will regularly assess and evaluate its methods and performance in relation to handling personal information

All management and staff are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

#### **Data collection: Informed consent**

Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with and the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.

We will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, we will ensure that the Data Subject:

- a) Clearly understands why the information is needed
- b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- e) Has received sufficient information on why their data is needed and how it will be used

**Please see Appendices for Informed Consent Form**

#### **Website Data Collection**

As part of Midos Management Co Ltd's collection of data there is a requirement for information to be requested, stored and processed directly from website communications.

As a result this data set will be supported as per the requirements of the Data Protection Act.

**Please see Appendices for Website Privacy Statement**

#### **Procedures for Handling Data & Data Security**

Under the data protection act 1998, companies and charities have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- unauthorised or unlawful processing of personal data
- unauthorised disclosure of personal data
- accidental loss of personal data

It is therefore important the all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

#### **Operational Guidance**

##### **Email:**

All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or, printed and stored securely. The original email should then be deleted from the



	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

personal mailbox and any “deleted items” box, either immediately or when it has ceased to be of use.

**Remember, emails that contain personal information which is no longer required for operational use, should be deleted from the personal mailbox and any “deleted items” box.**

#### **Phone Calls:**

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access.
- Personal information should not be given out over the telephone unless you have no doubts as the caller’s identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

#### **Laptops and Portable Devices:**

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program.

Ensure your laptop is locked (password protect) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of site, preferably in the boot.  
If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

#### **Data Security:**

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable) or processed for safe storage or disposal.

Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

#### **Passwords:**

Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

### **Protect Your Password:**

- Common sense rules for passwords are: do not give out your password
- do not write your password somewhere on your laptop
- do not keep it written on something stored in the laptop case

### **Data Storage**

Information and records relating to individuals will be stored securely and will only be accessible to authorised individuals.

- When data is stored on paper it should be kept in a secure place where unauthorised people cannot see it.
- When data is stored electronically it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is our responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

### **Data Accuracy**

The law requires Midos Management Co Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Midos Management Co Ltd will put into ensuring its accuracy.

It is the responsibility of the management and staff that work within data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few as places as necessary. Management and staff will not create any unnecessary additional data sets.
- Management and staff should take every opportunity to ensure data is updated. For example by confirming a customers' details when they contact
- Midos Management Co Ltd will make it easy for data subjects to update the information
- Midos Management Co Ltd holds about them. For example via the company website
- Data will be updated as inaccuracies are discovered. For example if a customer can no longer be reached on their stored telephone number, it will be removed from the data set

### **Information Regarding Employees or Former Employees**

Information regarding an employee or a former employee should be retained for an agreed 6 years . If something adverse does come up you might want to refer back to a job application or other piece of personal data within a document to check what was disclosed at the time.

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

The retention of data records has been agreed at management level to be 6 years for date of last entry.

### **Data Subject Access Requests**

All individuals who are the subject of personal data held by Midos Management Co Ltd are entitled to:

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

If an individual contacts the organisation requesting this information this is called a subject access request.

**Please see Appendices for procedure on Subject Access Request.**

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

### **Disclosing data for other reasons**

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the service to disclose data (including sensitive data) without the data subject's consent.

These are:

- a) Providing information in Safeguarding disclosures or to regulatory authorities in investigation of incident occurrence
- b) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person
- c) The Data Subject has already made the information public
- d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- e) Monitoring for equal opportunities purposes – i.e. race, disability or religion
- f) Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

We intend to ensure that personal information is treated lawfully and correctly.

### **Risk Management**

The consequences of breaching Data Protection can cause harm or distress to individuals if their information is released to inappropriate people, or they could be denied a service to which they are entitled. All management and staff should be aware that they can be personally liable



	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

if they use individuals' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the organisation is not damaged through inappropriate or unauthorised access and sharing.

**Please see Appendices for Data Protection Risk Analysis**

#### **Providing Information**

Midos Management Co Ltd aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights

To this purpose Midos Management Co Ltd has completed a privacy statement setting out how data relating to individuals is used by the company.

**Please see Appendices for Privacy Statement.**

#### **Further information**

If anybody including members of the public/or stakeholders have specific questions about information security and data protections in relation to Midos Management Co Ltd please contact the Data Protection Officer: Elizabeth Endzweig, Midos Management Co Ltd, 121-123 Clapton Common, London E5 9AB, or via email [elizabeth@midos.net](mailto:elizabeth@midos.net).

Or alternatively The Information Commissioner's website ([www.ico.gov.uk](http://www.ico.gov.uk)) is another source of useful information.

#### **Appendices**

- 1. Privacy Statement (Notice)**
- 2. Website Privacy Statement**
- 3. Informed Consent Form**
- 4. Breach Notification Procedure**
- 5. Data Protection Risk Analysis**

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

## Appendix 1 – Privacy Statement (Notice)

<b>Privacy Notice</b>	<b>Y</b>	<b>N</b>
The name and contact details of your organisation		
<b>Midos Management Co Ltd, 121-123 Clapton Common, London E5 9AB</b>		
The name and contact details of your GDPR Controller		
<b>Midos Management Co Ltd, 121-123 Clapton Common, London E5 9AB</b>		
The contact details of your Data Protection officer		
Elizabeth Endzweig		
The purposes of the processing		
To ensure we can carry out the duties of property management.		
The lawful basis for the processing		
Article 6(1)(c) of GDPR gives us a lawful basis for processing where:  <b>Legal obligation:</b> the processing is necessary for you to comply with the law (not including contractual obligations).		
The legitimate interests for the processing		
In order to carry out duties of property management it is required to hold personal data.		
The categories of personal data obtained		
The organisation holds personal information in order to carry out duties of property management including: <ul style="list-style-type: none"> <li>Names</li> <li>Date of Birth</li> <li>National Insurance Numbers</li> <li>Bank Details</li> <li>Any children/others residing at property</li> </ul>		
The recipients or categories of recipients of the personal data		
Management and staff of <b>Midos Management Co Ltd</b>		
The details of transfers of the personal data to any third countries or international organisations		
N/A with our data sets held		
The retention periods for the personal data		
Our records are retained for a period of 6 years following the last entry of data and then destroyed as per our Data Protection procedures on the safe disposal of records		
The rights available to individuals in respect of the processing		
The rights available to you are contained within our GDPR policy including: <ul style="list-style-type: none"> <li>Right to be informed</li> <li>Right of access</li> <li>Right to rectification</li> <li>Right to erasure</li> <li>Right to restrict processing</li> </ul>		

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

<ul style="list-style-type: none"> <li>• Right to data portability</li> <li>• Right to object</li> <li>• Rights related to automated decision making including profile</li> </ul>		
<b>The right to withdraw consent</b>		
The GDPR gives you specific right to withdraw consent. Should you choose to withdraw consent to the recording and maintaining of personal data in relation to your care service support then you can do this by contacting our GDPR Controller Elizabeth Endzweig on 0208 800 3366 or <a href="mailto:elizabeth@midos.net">elizabeth@midos.net</a>		
<b>The right to lodge a complaint with a supervisory authority</b>		
Should you wish to lodge a complaint with regards to your data protection and/or processing of personal data you can do so via the following: Information Commissioner's Office Tel: 0303 123 1113 Web: <a href="https://ico.org.uk/concerns/">https://ico.org.uk/concerns/</a>		
<b>The source of the personal data</b>		
Personal data will be recorded, kept in the following ways: <ul style="list-style-type: none"> <li>• Electronic systems</li> <li>• Paper documentation in secure locations</li> <li>• Archived documentation in both electronic and paper held in secure locations</li> <li>• Transferred via encrypted secure electronic systems</li> </ul>		
<b>The details of whether individuals are under a statutory or contractual obligation to provide the personal data</b>		
As you are required by law to provide personal data in completion of property rental we will only hold data specific to meeting this provision		
<b>The details of the existence of automated decision-making, including profiling</b>		
Automated decision making including profiling is not completed by our service		

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

## **Appendix 2 – Website Privacy Statement**

We are **Midos Management Co Ltd** a company incorporated in England and Wales. Our company number is **07721993** and our registered address is:

**123 Clapton Common, London E5 9AB**

**Midos Management Co Ltd (“we”/”our”/”us”)** are committed to ensuring that your privacy is protected. We will continue to comply with the provisions of the Data Protection Act (DPA) until 25 May 2018, after which we will comply with the General Data Protection Regulation ((EU) 2016/679 (GDPR) unless and until GDPR is no longer directly applicable in the UK, together with any national implementing laws, regulations and secondary legislation as amended or updated from time to time in the UK, and any successor legislation to GDPR and the DPA (together “Data Protection Legislation”). We are the data controller of data you pass to us pursuant to this policy. Our Data Protection Officer can be contract at [elizabeth@midos.net](mailto:elizabeth@midos.net) or 0208 800 3366..

### **Information you give to Midos Management Co Ltd**

You may give us information about you by completing enquiry forms on the website. The information you give us may include your name, email address/location and phone number.

We will retain this information while we are corresponding with you or providing service to you or to who you are representing. We will retain this information for 6 years.

Where we are processing personal data we have obtained via the website in the basis of having obtained consent from you, you have the right to object or withdraw your consent and can do so by contacting our Data Protection Officer on [elizabeth@midos.net](mailto:elizabeth@midos.net) or 0208 800 3366.. Please note however if you object or withdraw this may affect our ability to carry out the tasks detailed in the property management agreement.

We will not share, sell or distribute any of the information you provide to us (other than as set out in this policy) without your prior consent, unless required to do so by law.

### **How safe is your Information?**

Will we do our best to protect your personal data but the transmission of information via the Internet is not completely secure at all times. Any such transmission is therefore at your own risk.

### **Where we Store your Personal Data**

The data that we collect from you may be transferred to, and stored at, our head office. By submitting your personal data you agree to this transfer, storing or processing. We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Data Protection Policy.

No third parties have access to your personal data unless the law allow them to.

### **Statement on our Website**

#### **\*Important information about your data**

We value your privacy – Your information will be stored by Midos Management Co Ltd, registered company in England and Wales Company Number 07721963 and ICO Number

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

**ZA236733.** Your data will not be passed for 3<sup>rd</sup> party communications and you can revoke our access to your data at any time. You can refer to all Data Privacy information via our Data Protection Policy – [www.midos.net](http://www.midos.net).



	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

### Appendix 3 – Informed Consent Form

Name of Individual Tenant:

Address:

Midos Management Co Ltd - Data Protection Consent Form

#### Background

Midos Management Co Ltd uses your personal data for a number of different reasons. Personal data is any information that identifies you or, in some cases, information that is about you such as an opinion. It can include your name, email address, postal address, national insurance number and bank details.

We comply with the law in place in the UK around data protection when we use your personal data, which is known as "GDPR" (short for the General Data Protection Regulation). It allows us to use your personal data for a number of reasons without checking with you that it's ok for us to do so. For example, where we can show that we have legitimate reasons to use your personal data or where we need to use your personal data to provide us with the services you have requested from us, or to meet a legal obligation placed on us.

However, in some situations, we need you to confirm that you are happy for us to use your personal data. Please refer to our Data Protection Policy for further details.

#### Why we need your consent

We need your consent for us to carry out the following activities with your personal data: Holding of personal data in order to make contact and/or review our property management agreement with your home. We will keep this data for the length of the agreement and will destroy 6 years when this comes to an end.

#### What happens next?


If you are unsure about why we are processing your personal data for the reasons set out above, or what we are doing with it, please contact your Landlord. Please do not sign this form until you are happy that you understand its content.

If you give Midos Management Co Ltd consent to use your personal data in the ways explained above, you can ask Midos Management Co Ltd to stop using your personal data in this way at any time by speaking to Elizabeth Endzweig or by emailing us at [elizabeth@midos.net](mailto:elizabeth@midos.net), writing to us at 121-123 Clapton Common, London E5 9AB or phoning us on 0208 800 3366.

If you are happy for Midos Management Co Ltd to use your personal data in the ways set out above, please sign below

**Individual Name:**

ELIZABETH ENDZWEIG



**Date Signed:**

20/04/2018

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

## **Appendix 4 – Breach Notification Procedure**

### **What is a Breach?**

A breach of GDPR is any breach that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Examples of a breach may include:

- Sending an email to the incorrect recipient
- Copying rather than blind copying recipients of an email
- Losing a USB device containing personal data
- Leaving a hard copy of personal data (for example, a Service User record or employee file) in an easily accessible area so that details can be viewed or recorded, or the document taken
- Leaving a laptop or documents containing personal data on a train or other public transport; or
- Leaving a cupboard or filing drawer unlocked that contains personal data

Our process for Breaches are as follows:

### **Process Map Stage 1 - Log breach**

Midos Management Co Ltd understands that it should maintain a log of breaches. Midos Management Co Ltd will also record any potential breaches notified to it by employees or third parties which it determines not to be a breach, setting out its rationale for such a decision.

Midos Management Co Ltd will record the date of the breach, the date of notification of the breach (i.e. by the relevant employee) and actions taken in respect of the breach.

### **Stage 2 and 2a - Has the breach resulted in the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data?**

Midos Management Co Ltd recognises that not every breach of GDPR must be notified to the ICO. For example, there is no requirement to notify the ICO of a failure to respond to a Subject Access Request.

Midos Management Co Ltd understands that the notification requirements focus on the loss of, or unauthorised access to, personal data. Midos Management Co Ltd will therefore consider:

- Whether personal data has been affected by the breach (if, for example, only business data has been disclosed Midos Management Co Ltd understands that GDPR will not apply and there will be no requirement to notify the ICO); and
- Whether the personal data has been destroyed, lost, altered, disclosed or accessed as a result of the breach

Midos Management Co Ltd will record information about the breach and decisions taken for future reference. If there has been a security breach (irrespective of whether it requires notification to the ICO), Midos Management Co Ltd will consider whether, from a best practice perspective, it will proceed with Stages 4 and 5 to identify the cause of the breach and whether further steps can be taken to prevent further loss and disclosure of data (whether the data is personal data or otherwise).

### **Stage 3 - Identify the relevant team to investigate**

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

Midos Management Co Ltd anticipates that more than one team or individual may need to be involved or lead the investigation into the breach, and it will ensure that the appropriate people are involved at an early stage in the process.

#### **Stage 4 - Identify the cause of the breach and whether the breach has been contained**

Refer to further information at Stage 5.

#### **Stage 5 - Take all steps necessary to prevent further loss/disclosure**

Midos Management Co Ltd understands that the ICO must be notified within 72 hours of Midos Management Co Ltd becoming aware of the breach. Midos Management Co Ltd will also focus on ensuring that the breach is contained to prevent it worsening prior to notification. Midos Management Co Ltd will, where possible, notify the ICO in its initial notification of the steps it has already taken to mitigate the impact of the breach and will record all action it has taken.

#### **Stage 6 - Identifying if the breach is likely to result in a risk to the rights and freedoms of individuals**

Midos Management Co Ltd understands that the ICO must be notified of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. Midos Management Co Ltd recognises that guidance provided by the ICO explains that a breach is likely to result in a risk to the rights and freedoms of individuals if, left unaddressed, it is likely to have a significant detrimental effect on individuals in terms of, for example, discrimination against that individual, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Midos Management Co Ltd recognises that if the lost data is business personal data (i.e. individuals' work email addresses or phone numbers), it is unlikely that such loss will result in a risk to the rights and freedoms of those individuals, particularly if the information is publicly available elsewhere.

#### **Stage 6a - No need to take further action if response to Stage 6 is negative**

Although Midos Management Co Ltd may not be required to notify the ICO if there is no risk to the rights and freedoms of individuals, it should take steps to avoid a similar breach occurring in the future, particularly if a similar breach in the future could result in a risk to the rights and freedoms of individuals – see Stage 10.

#### **Stage 7 – Within 72 hours of becoming aware of the breach, notify ICO**

Midos Management Co Ltd understands that the ICO has provided a notification template for serious breaches under the Data Protection Act 1998 that should be notified to the ICO, and that the template is likely to be updated by the ICO prior to GDPR coming into force.

Midos Management Co Ltd will ensure that any breach notification it submits includes:

- The nature of each breach, including the categories and approximate numbers of individuals concerned and the categories and approximate numbers of personal data records concerned
- The name and contact details of the Privacy Officer/point of contact for the breach
- A description of the likely consequences of the breach; and
- A description of measures taken or proposed to be taken to deal with the breach and any measures taken to mitigate effects of the breach

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

Under the Data Protection Act 1998, the form should be sent to [casework@ico.org.uk](mailto:casework@ico.org.uk) with “DPA breach notification form” in the subject field or by post to: The Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Midos Management Co Ltd will review the relevant page on the ICO website to check whether the information around breach notification is updated in line with GDPR.

#### **Stage 8 - Consider whether affected individuals should be notified**

Midos Management Co Ltd understands that if the breach is likely to result in a “high” risk to the rights and freedoms of individuals, those individuals must be notified directly.

Midos Management Co Ltd recognises that the threshold is higher than the threshold for notifying the ICO. It should be determined on a case by case basis. Examples may be loss or disclosure of Special Categories of Personal Data, or the potential for significant financial impact.

If Midos Management Co Ltd is unable to notify affected Data Subjects individually (because, for example, of the number of Data Subjects affected), it will take out a public notice, for example in a national newspaper, informing affected individuals of the breach.

#### **Stages 9 and 9a - Notify data controller**

If Midos Management Co Ltd is acting as a data processor rather than a data controller, it will notify the relevant data controller of the breach. Midos Management Co Ltd will, if necessary, refer to the guidance note on ICO website entitled “GDPR - Key Terms” for further information.

#### **Stage 10 - Check if there is a risk of a future breach occurring**

Midos Management Co Ltd will have taken possible steps to mitigate the effect of the breach in accordance with Stage 5 above. Midos Management Co Ltd will also consider the breach more widely, in particular whether the breach could occur again and take the steps necessary to prevent such recurrence.

#### **Stage 11 - Consider whether further internal training or guidance for staff is necessary**

If the breach was caused by a member of staff, Midos Management Co Ltd will consider how and why the breach happened. Midos Management Co Ltd will consider whether further training or guidance would be beneficial, either for the member of staff or for the Organisation more widely.

#### **Stage 12 - Log all actions and decisions**

Midos Management Co Ltd will document all decisions taken in respect of any breaches, including whether or not to notify the ICO and/or affected individuals, steps taken to mitigate the breach and steps taken to prevent future recurrence and additional training. Midos Management Co Ltd will keep a record of all relevant dates and copies of relevant documents such as the initial report from the relevant member of staff and the notification to the ICO.

#### **Stage 13 - Action and log any related future correspondence from the ICO**

SERVICE NAME will record any correspondence it receives from the ICO in respect of breaches and comply with any suggestions and requirements of the ICO.

	<b>Data Protection Policy – Including GDPR requirements</b>	<b>April 2018</b>
--	---	-------------------

## **Appendix 5 – Data Protection Risk Analysis**

<https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>