Document ID MG-1-002-03	Title Data Protection Policy Suite	
Effective Date 19/01/2021	**Reviewed by** Paul David Munnelly	**Date Reviewed** 08/01/2024
	Approved by Paul David Munnelly	**Date Approved** 08/01/2024

Munnelly Group Ltd:

Data Protection Policy Suite

CONTENTS

1. Summary 3
2. The Academy 4
3. Data Protection 5
4. Right to Rectification, Erasure, Restriction of Processing & Data Portability Policy & Procedure 12
5. Right to Object Policy & Procedure 15
6. Right to Consent Withdrawal Policy & Procedure 17
7. Personal Data Breach Policy & Procedure 18
8. Data Security Policy 20
9. Clear Desk and Clear Screen/Screen Lock Policy 21
10. Password Strength Policy 22
11. Email & Digital Message Protection Policy 23
12. Bring Your Own Device Policy 25
13. Penetration Testing Policy 26
14. Physical Security Policy 27
15. Staff Training (Data Protection) Policy 28
16. Disaster/Incident Recovery Policy & Procedure 29
17. Data Retention and Destruction Policy 30

Document ID MG-1-002-03	Title Data Protection Policy Suite	
Effective Date 19/01/2021	**Reviewed by** Paul David Munnelly	**Date Reviewed** 08/01/2024
	Approved by Paul David Munnelly	**Date Approved** 08/01/2024

1. Summary

Designed with our Group and the various businesses in mind we have developed this policy suite to ensure that data we collect on behalf of our People, our Customers and our Communities is protected to the highest standards.
We have also developed our online training platform, The Munnelly Academy, which is a new way of integrating online learning into our Group.

With over 30 modules already developed, we use a blend of in-house content and industry standard content we have developed internally. We have created three key learning categories: legal and compliance, business skills and management and leadership. Each contains up-to-date content, relevant us, our diverse range of sectors and areas of work.

In addition, we have developed a number of stand-alone modules, focusing on specialist skills, perhaps relevant to only one department and can create custom content to meet any businesses specific needs.

What sets us apart is our market leading approach and our expertise. We are not interested in what our competitors do; **we lead and do not follow.**

The Munnelly Academy aims to help you, our People, navigate their career and ensure that we invest in you.

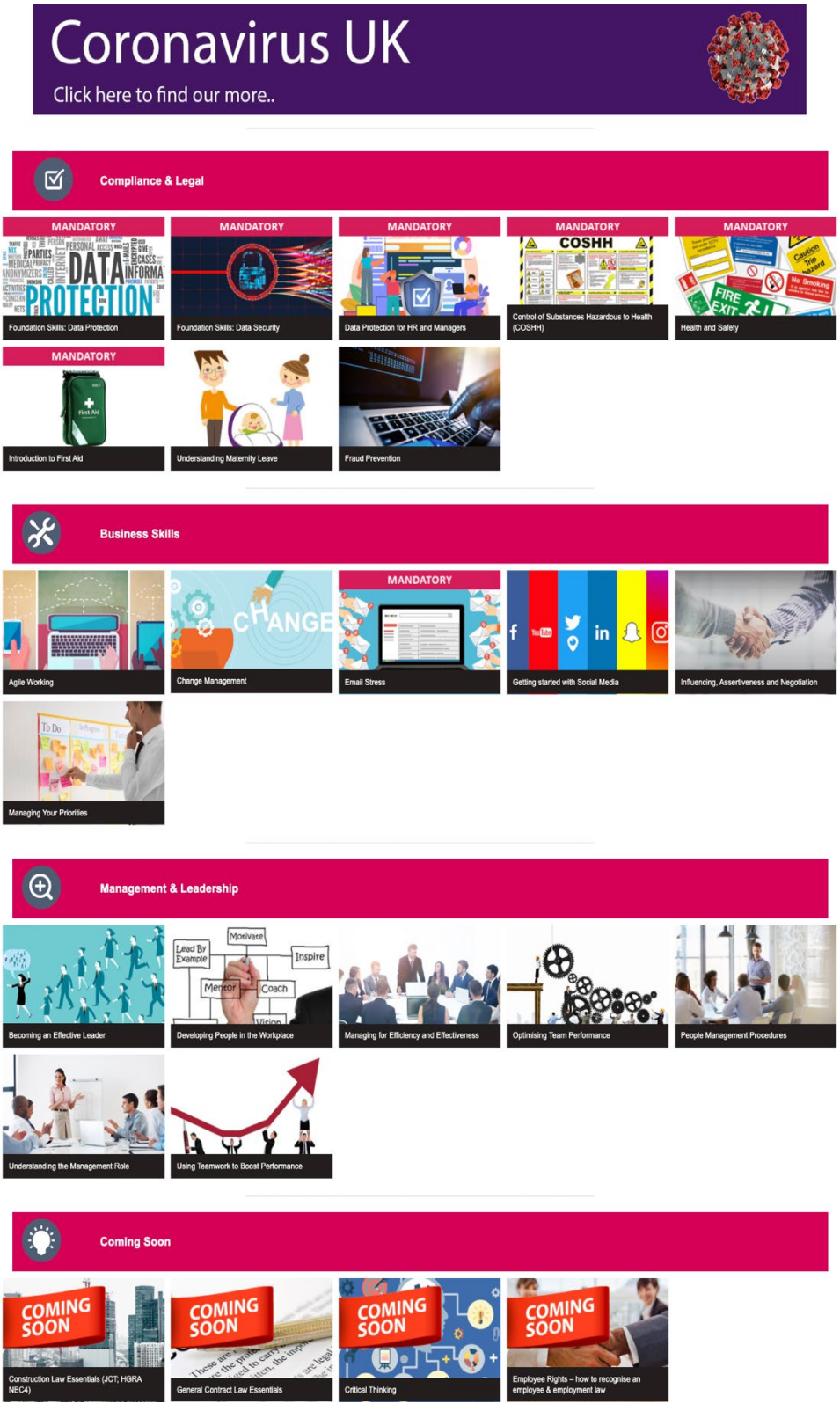
We have updated our training modules to take into account the current COVID-19 epidemic and will continue to develop our processes and systems.

Questions in relation to this policy must be directed to **DPO@munnellys.com.**

Questions in relation to The Munnelly Academy must be directed to HR@munnellys.com

2. The Academy

The below are provided via The Academy. Core modules must be completed as directed.



3. Data Protection

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Contents

1. Introduction
2. Key points to remember
3. Key definitions
4. The Principles
5. Lawful bases for processing
6. Consent
7. Direct marketing
8. Special Categories of data
9. Fair processing information
10. Data Subject rights
11. Fees, verifying identity, time limits and exemptions
12. Law enforcement requests
13. Third party processors
14. Records of data processing activities
15. Data retention
16. Security
17. Data breaches
18. Data Protection Impact Assessments
19. Data Protection by Design
20. International transfer of personal data
21. Training
22. Complaints
23. Derogations

Introduction

As part of our day to day business activities, we obtain information (including personal data) about individuals (data subjects). This includes personal data relating to our employees, customers, third party processors and individuals who work for other organisations such companies within our group. The law requires us to implement certain measures to protect the rights that these individuals have in respect their personal data and how it is handled. It is of crucial importance to the business to ensure that personal data and other confidential information is kept safe and only processed in accordance with the law. This policy summarises the law on data protection and explains how personal data must be processed by the company in order to ensure compliance the law. This policy should be read in conjunction with the other policies contained within our Data Protection Policy Suite.

Key points to remember

- **If you are unsure about anything in this policy or if you are uncertain about a specific issue relating to the handling/processing of personal data, then you should contact Group Legal and / or HR for guidance.**
- **The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 are, at present, the key pieces of legislation that govern personal data processing in the United Kingdom.**

Key definitions

The following important terms are defined by the GDPR and may assist you when reading and understanding this policy as well as the various other policies and procedures contained within our Data Protection Policy Suite:

- **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

- **'profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

- **'pseudonymisation'** means 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 are not attributed to an identified or identifiable natural person;

- **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

- **'controller'** means 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;

- **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

- **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

- **'consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

- **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- **'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

- **'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;

- **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

The Principles

The GDPR provides a number of **Principles** which must be adhered to when processing personal data. All staff must be aware of the Principles and always try to ensure that personal data is never processed in a manner that it incompatible with the Principles. The law states that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject **('lawfulness, fairness and transparency')**;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; **('purpose limitation')**;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **('data minimisation')**;
- 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 **('accuracy')**;
- 2kept 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; **('storage limitation')**;
- 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 **('integrity and confidentiality')**;
- In addition, the law provides that we, as a controller of personal data, shall also be responsible for, and be able to demonstrate compliance the above Principles **('accountability')**.

Lawful bases for processing

The GDPR provides that processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- 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 the data subject prior to entering into a contract;
- processing is necessary for compliance with a **legal obligation** to which the controller is subject;
- processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
- 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;
- 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 or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

We must ensure that we only ever process personal data where at least one of the above lawful bases apply to that processing. If you are unsure about whether an activity you are about to perform on personal data is covered by one of the above lawful bases, you should seek guidance from **Group Legal and / or HR** before carrying out the processing.

Consent

The GDPR provides that, where processing is based on '**consent**', we must be able to demonstrate that the data subject has consented.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which does not comply with this requirement will not be binding.

The data subject has the right to withdraw his or her consent at any time, however, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed of the fact that they have the right to withdraw their consent at any time. It must be easy for the data subject to withdraw their consent.

We will notify data subjects of their rights relating to consent. In most cases, this will be done within the Privacy Notices that we provide to data subjects. However, if we are processing any personal data on the basis of consent, we must always be aware of the data subject's right to withdraw consent. If a data subject withdraws their consent, you must cease processing their personal data and seek immediate guidance from **Group Legal and / or HR**.

Direct marketing

In the event that we engage in any form of direct marketing, we must ensure that any marketing material sent to individuals (i.e. where we process the individual's personal data in order to send a marketing message) complies with both the GDPR and the Privacy and Electronic Communications Regulations (PECR).

Any direct marketing based on the 'consent' of the data subject must comply with the above requirements. Similarly, any direct marketing based on 'legitimate interests' must comply with the specific requirements of the PECR.

You must not engage in any direct marketing activities such as sending marketing emails directly to data subjects without prior authorisation from **Group Legal and / or HR**.

Special Categories of data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is **prohibited** under the GDPR.

The GDPR states that such 'special category data' (formerly known as 'sensitive personal data') **may only be processed if one of the following applies**:

- the data subject has given **explicit consent** to the processing for one or more specified purposes – except in any circumstances where the law provides that they cannot give such consent;

- processing is necessary for the purposes of **carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law**;

- processing is necessary to **protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

- processing is carried out in the course of its **legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates

solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

- processing relates to personal data which are **manifestly made public** by the data subject;
- processing is necessary for the **establishment, exercise or defence of legal claims** or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of **substantial public interest**;
- processing is necessary for the purposes of **preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services**;
- processing is necessary for reasons of **public interest in the area of public health – in particular relating to pandemic and epidemics and areas of significant national importance and emergency**;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

You must **not** process special categories of data without prior written authorisation from **Group Legal and / or HR**.

Fair processing information
The GDPR provides that, where personal data is collected from the data subject, we must, at the time when personal data are obtained, provide the data subject with all of the following information:

- Our identity and contact details;
- the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- where the processing is based on 'legitimate interests', details of those interests;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that we intend to transfer personal data to a third country or international organisation and details of the appropriate safeguards that we will use to protect the personal data and how the data subject can obtain further details if they wish to;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from us access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time (if applicable);
- the right to lodge a complaint with the Information Commissioner's Office (ICO);
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

We will achieve this by providing data subjects with a Privacy Notice at the appropriate time. We may update our Privacy Notices as and when required – including in circumstances where we intend to process personal data that we have already obtained from a data subject for another purpose i.e. a purpose other than that for which the personal data was originally collected. Such updated versions will be provided to the data subject prior to any such further processing.

Data Subject rights
The GDPR provides data subjects with a number of specific rights in respect of their personal data. Details of these rights and how we are to respond to requests from data subjects seeking to enforce their rights ("requests") are detailed in separate policies. You should familiarise yourself with these policies, however, the rights that data subjects have are as follows:

- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object/including right to object to automated decision making
- Right to Withdraw Consent
- Right to Complain to the ICO

Fees, verifying identity, time limits and exemptions
Generally, we are required to respond to requests received from data subjects free of charge, however, there are circumstances where it may be appropriate to charge a fee – for example, where the data subject requests additional copies of documents previously provided to them under the right of access or where we have chosen to respond to a request that is "excessive" or "manifestly unfounded". Any fees charged will be limited to administrative costs and will be determined by **Group Legal and / or HR**.

If there is any doubt with regards to the identity of the person making the request or where the request is being made on behalf of another person, it may be necessary for us to request proof of identity prior to responding to the request. This will be determined in each case by **Group Legal and / or HR**.

We must respond to requests received from data subjects without undue delay and no later than one month from the date that the request was received. For example, if a request is received on 1st March, the data subject must receive our response no later than 1st April. It is possible to extend this time period by up to two further months (i.e. three months in total from the date of receipt) where necessary taking into account the "complexity" and "number of requests". The timeframe for responding will, in each case, be determined by [**Group Legal and / or HR**.

When responding to requests, **Group Legal and / or HR** will be responsible for determining whether any exemptions apply under the law which might permit us to either refuse a request or, where – for example – the request is made under the right of access, refuse to disclose certain documents to the data subject. An example of such an exemption is where documentation contains the personal data of a third party or other exempt information such as legal advice or confidential references.

Law enforcement requests
As an organisation, we may sometimes receive official requests for information about individuals from law enforcement agencies and other statutory bodies such as the police, regulators or HM Revenue and Customs.

It may be necessary in such situations, and in certain specific circumstances, for us to share information about individuals – including employees or customers –with those agencies. This could be in response to a request for information received from a law enforcement agency or, where necessary, an unsolicited disclosure of information made at the company's discretion. This can be done without the data subject's knowledge or consent. In most cases, this will be in response to a request from an agency that relates to the prevention or detection of crime, the apprehension or prosecution of offenders, the assessment or collection of a tax or duty by order of a court or by any rule of law. Any requests received from law enforcement agencies or other organisations must be forwarded immediately to **Group Legal and / or HR** who will be responsible for considering the request and responding on behalf of the company should we choose to do so. Employees should **not** respond to the agency/organisation themselves. This should only be done on behalf of the company by **Group Legal and / or HR**.

Third party processors
It will sometimes be necessary for us to transfer personal data to other third-party organisations who perform services for us or on our behalf. When it is necessary to transfer personal data to such organisations to enable them to provide their services, the law requires us to enter into a written agreement with them that makes adequate provision for the protection of the personal data transferred. We will only transfer personal data to third party organisations where they have provided us with sufficient guarantees concerning their own compliance with the GDPR and where we have entered into a written agreement making provision for the processing of personal data. You must not transfer personal data to another organisation unless we have a prior agreement in place with them. If you are in any doubt about this, you should seek guidance from **Group Legal and / or HR** before transferring any personal data.

Record of data processing activities
We will maintain a written record of all of the personal data processing activities that the business engages in. **Group Legal and / or HR** will be responsible for updating and maintaining this record.

Data retention
We must ensure that we do not retain personal data for longer than is necessary. Our Data Retention Policy will determine for how long we retain personal data by category. Personal data that is no longer required by the business will be permanently deleted in accordance with the policy. Personal data must only ever be deleted in accordance with the Data Retention Policy or following an approved request from a data subject under the Right to Erasure. Right to Erasure requests may only be dealt with by **Group Legal and / or HR** who will be responsible for ensuring the erasure of any personal data following an approved erasure request.

Security

We will implement appropriate technical and organisational measures in order to ensure a level of security, for the protection of personal data, which is appropriate to the risk. Our Data Security Policy set out details of the steps that we must take to protect personal data and confidential information. You should familiarise yourself with the Data Security Policy and ensure that you adhere to it at all times. Queries about the policy should be directed to **Group Legal and / or HR.**

Data breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Our Personal Data Breach Policy and Procedure details what the GDPR says an organisation must do and what steps you must take in the event of a data breach or suspected data breach. You should familiarise yourself with the Data Breach Policy and ensure that you adhere to it in the event of a breach or suspected breach.

It is important to remember that such events must be reported and acted upon immediately. Some examples of events that could amount to a personal data breach are:

- Sending an email containing personal information about an employee or customer to the wrong person;
- A cyber-attack where hackers gain access to our network;
- Leaving documents containing personal data unattended;
- Theft/loss of a company laptop, mobile phone, USB or other device containing personal data;
- Allowing unauthorised persons to enter company premises.

Data Protection Impact Assessments

The law requires us to conduct a Data Protection Impact Assessment (DPIA) where we are planning to engage in any personal data processing activities (particularly where new technologies are to be used) that are likely to result in a **high risk** to the rights and freedoms of individuals. A DPIA is an assessment of the impact of the envisaged processing operations on the protection of personal data.

We will conduct a DPIA in any situation where we are planning to process personal data in a manner which might present a high risk to the rights and freedoms of individuals and, in particular, where the proposed processing involves:

- systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or
- systematic monitoring of a publicly accessible area on a large scale.

The DPIA will contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, any legitimate interests that we might rely on as a basis for processing;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The person responsible for conducting DPIA's for the business is **Group Legal and / or HR**.

Data Protection by Design

Where a DPIA is not required by law, we will nevertheless ensure that we adhere to the principle of Data Protection by Design. This means that when we determine the means of personal data processing by the business and whilst we are engaged in personal data processing, we will implement appropriate technical and organisational measures which are designed to implement data protection principles in an effective manner and in a way that respects and observes the data protection rights of data subjects and which ensures compliance with the requirements of the GDPR.

International transfer of personal data

No member of staff must allow personal data to be transferred to any individual or organisation located outside the European Economic Area (EEA) without the prior written approval of **Group Legal and / or HR**.

Group Legal and / or HR will determine whether it is possible to conduct the transfer and what safeguards may be required in order to protect personal data during the transfer.

If you are unsure about any aspect of an international transfer of personal data, if you are uncertain as to whether a transfer you are about to make amounts to an international transfer of personal data or if you are unsure as to whether the recipient country/organisation is outside the EEA, you should seek immediate guidance from **Group Legal and / or HR**, prior to carrying out the transfer.

Training
All staff will receive data protection training in accordance with the Staff Training (Data Protection) Policy.

Complaints
Any complaints relating to data protection issues should be immediately directed to Group HR and / or Legalwho will be responsible for conducting an investigation. You should confirm receipt with Group HR and / or Legalif forwarding a complaint.

Group Legal and / or HR will inform the complainant of the progress and the outcome of their complaint within a reasonable time period.

In the event that the complainant is not satisfied following our internal investigation, we will remind the complainant of their right to complain directly to the Information Commissioner's Office (ICO).

Derogations
Any derogations from the requirements of this policy, or any other policy within the company's Data Protection Policy Suite, shall require prior written approval from **Group Legal and / or HR.**

4. Right to Rectification, Erasure, Restriction of Processing & Data Portability Policy & Procedure

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must be able to recognise a Rectification, Erasure, Restriction of Processing and Data Portability Request.**
- **You must pass such requests on quickly to Group HR and / or Legal.**
- **You must know what information to pass to Group HR and / or Legal.**
- **You must follow any instructions given to you by Group HR and / or Legal in response to such requests**

Introduction

The General Data Protection Regulation (GDPR) provides individuals (known as "data subjects") with the following additional rights in respect of their personal data:

1. The right to rectification
2. The right to erasure
3. The right to restriction of processing
4. The right to data portability

The **right to rectification** provides the data subject with the right to obtain from the data controller without undue delay the rectification of any inaccurate personal data concerning him or her. The data subject also has the right to have incomplete personal data completed – including by means of providing a supplementary statement.

The **right to erasure** (sometimes referred to as the "right to be forgotten") provides the data subject with the right to obtain from the data controller the erasure of personal data concerning him or her without undue delay. The right to erasure, however, is not an absolute right and there are exemptions which may apply – depending on the circumstances – which means that we would be entitled to refuse such a request – for example, where we were under a legal obligation to retain the data.

When must we erase?

In instances, where the personal data must be erased, the controller is obligated to erase the personal data without undue delay where one of the following grounds apply:

1. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

2. the data subject withdraws consent on which the processing is based and where there is no other legal basis for the processing;

3. the data subject objects to the processing and there are no overriding legitimate grounds for the processing or the data subject objects to the processing pursuant to the right to object;

4. the personal data have been unlawfully processed;

5. the personal data have to be erased for compliance with a legal obligation;

6. the personal data have been collected in relation to the offer of information society services.

Other steps that may be necessary

The law also states that, where a controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

When will the right to erasure not apply?

The law states that the right to erasure does not apply to the extent that the processing of the personal data is necessary for:

1. exercising the right of freedom of expression and information;

2. compliance with a legal obligation which requires processing by law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

3. reasons of public interest in the area of public health;

4. archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

5. the establishment, exercise or defence of legal claims

The **right to restriction of processing** states that a data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

1. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

2. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

3. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

4. the data subject has objected to processing pending the verification of whether the legitimate grounds of the controller override those of the data subject.

In what circumstances can the data be used without consent?
The law states that where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. A data subject who has obtained restriction of processing shall then be informed by the controller before the restriction of processing is lifted.

Communicating rectification or erasure to others
The law also states that a controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller must inform the data subject about those recipients if the data subject requests it.

The **right to data portability** states that the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to have that personal data transmitted to another controller without hindrance, where:

1. the processing is based on consent or on a contract; and

2. the processing is carried out by automated means.

In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. Complying with a request made under the right to data portability must not adversely affect the rights and freedoms of others.

Does the request have to state clearly what type of request it is?
It is important to remember that requests made by data subjects in respect of their above mentioned rights do <u>not</u> have to be entitled or contain the words "Right to Erasure Request" or similar. A valid request can be made if an individual makes such a request even if they do not make explicit reference to the name of the right as it appears in the GDPR. Requests can be received verbally or by letter, email, social media message or any other type of communication.

Responding to a request
Upon receipt of a Request, the data controller is required to respond without undue delay and, in any event, within one month of receipt of the request. This period may be extended by two further months where necessary taking into account the complexity and number of requests. Such extensions must be communicated to the data subject within one month of receipt of a request.

What might happen if we fail to respond to a request or respond late?
Failure to adequately respond to a Request is likely to be regarded as a breach of the GDPR and could result in Macrail Systems Ltd having to pay (i) compensation and legal costs to either an individual data subject or a group of data subjects as part of a class action the and/or (ii) a financial penalty to the Information Commissioner. Other possible consequences could include an ICO investigation, public censure or unwanted media coverage. The Information Commissioner has the power to impose a financial penalty of up to 4% of our annual global group turnover or the equivalent of 20 million EURO – whichever is greater. Alternatively, the ICO could issue an enforcement notice. It is, therefore, very important that the following procedure is followed in all instances where one of the above Requests is received.

If you are in any doubt as to whether you have received a Request, you should contact **Group HR and / or Legal** immediately.

Procedure to follow
The following steps **MUST** be followed when a Request is received.

1. If you receive a verbal or written (letter, email, social media or any other form of communication) request that amounts to (or which you think may amount to) a Request, you must notify **Group HR and / or Legal** immediately and certainly no later than 1 working day following receipt of the request. If possible, you should do this by sending an email to **Group HR and / or Legal** at the following email address: **DPO@munnellys.com** and confirm receipt with them.

2. If the Request was made verbally (in person or on the telephone), you should notify **Group HR and / or Legal** by sending an email to **DPO@munnellys.com** containing the following information:

   NAME OF PERSON MAKING THE REQUEST:
   REQUEST MADE ON BEHALF OF (if applicable):
   DATE OF REQUEST:
   TIME OF REQUEST:
   HOW WAS THE REQUEST MADE?:
   NATURE OF THE REQUEST (e.g. Erasure Request)
   NOTE OF WHAT WAS SAID:
   CONTACT DETAILS FOR THE PERSON MAKING THE REQUEST:

3. If the request was received electronically, you must forward/attach a copy of the request to the email to **Group HR and / or Legal.**

4. If the request was received by letter or other hard copy communication, you should ensure that the hard copy is forwarded to **Group HR and / or Legal** by **DPO@munnellys.com.**

5. Once **Group HR and / or Legal** has received notification of the request, they will record the relevant details of the request on to the **DPO@munnellys.com**.

6. **Gropu HR and / or Legal** will make contact in writing with the data subject, in order to acknowledge receipt of the request and confirm the date on which a response will be provided. **Group HR and / or Legal** will aim to send this letter to the data subject within 2 working days of receiving the notification.

7. **Group HR and / or Legal** will then be responsible for coordinating the necessary search for the relevant data.

8. If **Group HR and / or Legal** considers that additional time (beyond one month) is likely to be required in order to provide a response owing to the complexity and/or number of requests, then he/she will notify the data subject accordingly, providing reasons for the decision and providing a date for the response (up to three months from the date that the request was first received by the company).

9. Once all data that falls within the scope of the request has been collated, **Group HR and / or Legal** will conduct a review of the data to determine the following:

   a. Which of the data falls within the scope of the request;
   b. Whether any exemptions or other factors apply which mean that the request cannot be granted or can only be granted in part;
   c. Any other relevant issues.

Group HR and / or Legal will then make a final decision regarding the request and prepare a response to the data subject and update the **Request Register** accordingly. The **Request Register** will be updated by **Group HR and / or Legal** at regular intervals and as required throughout the above process.

5. Right to Object Policy & Procedure

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must be able to recognise when someone is objecting to the processing of their personal data**
- **You must pass such objection notifications on quickly to Group HR and / or Legal**
- **You must know what information to pass to Group HR and / or Legal**
- **You must follow any instructions given to you by Group HR and / or Legal in response to such notifications**

Introduction

The General Data Protection Regulation (GDPR) provides individuals (known as "data subjects") with the right to object, on grounds relating to his or her particular situation and at any time, to the processing of personal data concerning him or her which is based on any processing that is carried out on the basis of "public interest" or "legitimate interests" including profiling. Upon receipt of such a request, the controller shall no longer process the personal data unless they are able to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. These issues will be determined by Group HR and / or Legal, however, it is important that you are able to recognise a request received under the right to object and ensure that you adhere to the procedure set out below.

Examples:

Objection to marketing

Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of their personal data for such marketing. This may include profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data must no longer be processed for such purposes.

Objection to automated decision making

In addition, a data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision:

1. is necessary for entering into or performance of a contract between the data subject and the data controller;
2. is authorised by 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; or
3. is based on the data subject's explicit consent.

Does the request have to say what type of request it is?

It is important to remember that request made by a data subject in respect of their above mentioned right does not have to be entitled or contain the words "Right to Object Request" or similar. A valid request can be made if an individual makes such a request even if they do not make explicit reference to the title of the right as it appears in the GDPR. Requests can be received verbally or by letter, email, social media message or any other type of communication.

Responding to the request

Upon receipt of a Request, the data controller is required to respond without undue delay and, in any event, within one month of receipt of the request. This period may be extended by two further months where necessary taking into account the complexity and number of requests. Such extensions must be communicated to the data subject within one month of receipt of a request.

What happens if we fail to respond to the request or respond late?

Failure to adequately respond to a Request is likely to be regarded as a breach of the GDPR and could result Macrail Systems Ltd having to pay (i) compensation and legal costs to either an individual data subject or a group of data subjects as part of a class action the and/or (ii) a financial penalty to the Information Commissioner. Other possible consequences could include an ICO investigation, public censure or unwanted media coverage. The Information Commissioner has the power to impose a financial penalty of up to 4% of our annual global group turnover or the equivalent of 20 million EURO – whichever is greater. Alternatively, the ICO could issue an enforcement notice. It is, therefore, very important that the following procedure is followed in all instances where one of the above Requests is received.

If you are in any doubt as to whether you have received a Request, you should contact **DPO@munnellys.com** immediately.

Procedure to follow

The following steps **MUST** be followed when a Request is received.

1. If you receive a verbal or written (letter, email, social media or any other form of communication) request that amounts to (or which you think may amount to) a Request, you must notify **DPO@munnellys.com** immediately and certainly no later than 1

working day following receipt of the request. If possible, you should do this by sending an email to **DPO@munnellys.com** at the following email address: **DPO@munnellys.com** and confirm receipt with them.

2. If the Request was made verbally, you should notify **DPO@munnellys.com** by sending an email to **DPO@munnellys.com** containing the following information:

   NAME OF PERSON MAKING THE REQUEST:
   REQUEST MADE ON BEHALF OF (if applicable):
   DATE OF REQUEST:
   TIME OF REQUEST:
   HOW WAS THE REQUEST MADE?:
   NATURE OF THE REQUEST (e.g. Right to Object Request)
   NOTE OF WHAT WAS SAID:
   CONTACT DETAILS FOR THE PERSON MAKING THE REQUEST:

3. If the request was received electronically, you must forward/attach a copy of the request to the email to **DPO@munnellys.com.**

4. If the request was received by letter or other hard copy communication, you should ensure that the hard copy is forwarded to **Group Legal** by **DPO@munnellys.com.**

5. Once **Group Legal** has received notification of the request, **They** will record the relevant details of the request on to the **Request Register**.

6. **DPO@munnellys.com** will make contact in writing with the data subject, in order to acknowledge receipt of the request and confirm the date on which a response will be provided. **DPO@munnellys.com** will aim to send this letter to the data subject within 2 working days of receiving the notification.

7. **DPO@munnellys.com** will then be responsible for coordinating the necessary search for the relevant data.

8. If **DPO@munnellys.com** considers that additional time (beyond one month) is likely to be required in order to provide a response owing to the complexity and/or number of requests, then he/she will notify the data subject accordingly, providing reasons for the decision and providing a date for the response (up to three months from the date that the request was first received by the company.

9. Once all data that falls within the scope of the request has been collated, **DPO@munnellys.com** will conduct a review of the data to determine the following:

   a. Which of the data falls within the scope of the request
   b. Whether any exemptions or other factors apply which mean that the request cannot be granted or can only be granted in part
   c. Any other relevant issues

DPO@munnellys.com will then make a final decision regarding the request and prepare a response to the data subject and update the **Request Register** accordingly. The **Request Register** will be updated by **DPO@munnellys.com** at regular intervals and as required throughout the above process.

6. Right to Consent Withdrawal Policy & Procedure

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must be able to recognise when someone is withdrawing their consent to personal data processing**
- **You must pass such notifications on quickly to Group HR and / or Legal**
- **You must know what information to pass to Group HR and / or Legal**
- **You must follow any instructions given to you by Group HR and / or Legalin response to such notifications**

Introduction

In order for the business to process personal data, we must have a lawful basis on which to do so. More information on the lawful bases for processing can be found in the Data Protection Policy. One of the lawful bases for processing can be where the data subject has provided their consent. However, where processing takes place on the basis of consent, the data subject has the right to withdraw their consent at any time. If a data subject withdraws their consent to the processing of their personal data, we must cease processing immediately unless we are able to rely on an alternative basis for processing instead (e.g. for the performance of a contract or in order to comply with a legal obligation etc). If you are in doubt about this when carrying out your day to day tasks for the business, you should seek guidance from Group HR and / or Legal before continuing to process the data.

When might this be particularly relevant?

This may also affect any personal data processing that the business undertakes on the basis of 'legitimate interests'. Whilst legitimate interests can sometimes be relied upon as a valid basis for processing personal data, such processing must be balanced against the rights of the data subject. If a data subject withdraws their consent to personal data processing, there is a good chance that this will also prevent us from continuing to process the personal data on the basis of 'legitimate interest' given that the withdrawal of consent is often a strong indication that the rights/wishes of the individual now outweigh the interests of the business in processing the personal data in question.

This will be of particular relevance in circumstances where the business processes personal data on the basis of legitimate interests or where we are engaged in direct marketing and/or profiling.

Procedure to follow

Should a data subject inform us that they have withdrawn their consent to personal data processing, you must immediately notify Group HR and / or Legal, provide the following information and confirm receipt with them:

NAME OF PERSON WITHDRAWING CONSENT:
REQUEST MADE ON BEHALF OF (if applicable):
DATE OF REQUEST:
TIME OF REQUEST:
HOW WAS THE REQUEST MADE?:
NOTE OF WHAT WAS SAID:
CONTACT DETAILS FOR THE PERSON MAKING THE NOTIFICATION:

Group HR and / or Legal will then be responsible for reviewing the data processing activities relating to the data subject, making the necessary decision as to whether processing of personal data can continue under an alternative basis and taking any necessary follow up steps.

7. Personal Data Breach Policy & Procedure

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must know what circumstances are likely to amount to a personal data breach**
- **You must notify Group HR and / or Legal immediately and as a matter of urgency when you discover that a personal data breach has occurred**
- **You must know what information to pass to Group HR and / or Legal**
- **You must follow any instructions given to you by Group HR and / or Legal in response to such requests**
- **You must understand what would amount to a "near miss" and notify Group HR and / or Legal whenever such near misses occur**

Introduction

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What we must do

The law states that, in the case of a personal data breach, the controller must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office (ICO), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural (living) persons.

A personal data breach that is likely to present a risk to the rights and freedoms a data subject is one where, if not addressed in an appropriate and timely manner, could result in physical, material or non-material damage to persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the person concerned.
If notification to the ICO is not made within 72 hours, it must be accompanied by reasons for the delay.
In any instances where Macrail act as a processor of personal data for another controller, we will be required to notify the controller (i.e. NOT the ICO) without undue delay after becoming aware of a personal data breach involving their personal data.

What must the notification include?

The law requires that any notification to the ICO must at least:

1. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

3. describe the likely consequences of the personal data breach;

4. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay. We must document any personal data breaches – recording the facts, its effects and the remedial action taken.

When must we notify the data subject(s)?

When a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller shall communicate the personal data breach to the data subject without undue delay. The communication to the data subject must describe in clear and plain language the nature of the personal data breach and at least:

1. communicate the name and contact details of the data protection officer [ENTER NAME OF DPO] or other contact point Group HR and / or Legalwhere more information can be obtained;
2. describe the **likely** consequences of the personal data breach;
3. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Communication to the data subject is **not** required if any of the following conditions are met:

1. We, as the controller, have implemented appropriate technical and organisational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

2. We have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
3. It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

What is "high risk" breach?
The business will consider the following as amounting to a "high risk" personal data breach that is likely to require reporting to the ICO and/or the data subject(s) affected:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed) that is likely to cause physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

Procedure to follow

Failure to adequately respond to a personal data breach is likely to be regarded as a serious breach of the GDPR and could result Macrail Systems Ltd having to pay (i) compensation and legal costs to either an individual data subject or a group of data subjects as part of a class action the and/or (ii) a financial penalty to the Information Commissioner. Other possible consequences could include an ICO investigation, public censure or unwanted media coverage. The Information Commissioner has the power to impose a financial penalty of up to 4% of our annual global group turnover or the equivalent of 20 million EURO – whichever is greater. Alternatively, the ICO could issue an enforcement notice. It is, therefore, very important that the following procedure is followed in all instances where a data breach occurs or is suspected to have occurred.

The following procedure **MUST** be followed by all members of staff who become aware of a personal data breach that has occurred or suspect that a personal data breach may have occurred. If you are in any doubt as to whether a personal data breach has occurred in a particular situation, you should contact **DPO@munnellys.com** immediately and seek advice.

1. Notify **DPO@munnellys.com** immediately. You can do this by sending an email to **DPO@munnellys.com** and confirming receipt with Group HR and / or Legal. If you send an email, you should include the following information:

   DETAILS OF THE BREACH OR SUSPECTED BREACH INCLUDING THE CIRCUMSTANCES, A DESCRIPTION OF THE PERSONAL DATA INVOLVED AND HOW THE BREACH OCCURED:
   DATE & TIME OF THE BREACH:
   DATE & TIME THAT YOU (OR ANOTHER) DISCOVERED THE BREACH:
   DETAILS OF WHO DISCOVERED THE BREACH:
   ANY OTHER RELEVANT INFORMATION:
   REASONS FOR ANY DELAY IN REPORTING THE BREACH TO DPO@munnellys.com:

2. Once **Group Legal** has received notification of the breach/suspected breach, **they** will record the relevant details on to the **Breach Register**

3. **DPO@munnellys.com** will then investigate the breach/suspected breach.

4. Once **Group Legal** has carried out an initial investigation, **they** will determine whether a personal data breach has occurred and, if so, whether it is necessary to report the breach to the ICO and/or the data subject(s) with reference to the above mentioned criteria. **Group Legal** will then update the **Breach Register** accordingly. If a personal data breach has not occurred but **Group Legal** concludes that a "near miss" has occurred, **they** will record details of the near miss on the **Near Miss Register**.

5. **DPO@munnellys.com** will then determine any further steps that are necessary in response to the personal data breach/suspected personal data breach and record these in the appropriate register.

DPO@munnellys.com will be responsible for reviewing the **Breach and Near Miss Registers** at **three monthly**intervals to evaluate and determine whether any action is necessary in order to improve personal data security. Such steps will be recorded in writing.

8. Data Security Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Contents

1. **Clear Desk & Clear Screen/Screen Lock Policy**
2. **Password Strength Policy**
3. **Email & Digital Message Protection Policy**
4. **Bring Your Own Device Policy**
5. **Penetration Testing Policy**
6. **Physical Security Policy**
7. **Staff Training (Data Protection) Policy**
8. **Disaster/Incident Recovery Policy & Procedure**

9. Clear Desk and Clear Screen/Screen Lock Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must know what amounts to personal data and confidential information and ensure that such data is stored away when not in use**
- **All portable data storage and computing devices must be stored in a locked location when not in use.**
- **When leaving a computer for any period of time the screen must be locked**
- **Any material that is printed must not be left unattended**
- **If confidential information is found unattended in any location it must be immediately secured.**

Introduction

This policy describes how personal data and other confidential information should be handled when a working area is left unattended. The purpose of this is to ensure that the working area and the personal data/confidential information being used is protected from loss, unlawful disclosure or theft.

It is the responsibility of each employee to make every effort to ensure that personal data and other important information is held in a secure manner. Maintaining a clear desk and clear screen can help to protect personal data and other confidential information by reducing the threat of security breaches. Material that is left exposed and unattended represents a security risk and is susceptible to damage, unlawful disclosure or theft. This includes other business assets (e.g. laptops and mobile phones etc) and information left visible on computer screens, tablets and mobile phones. Failure to take appropriate measures aimed at protecting against the unauthorised access to or theft of personal data is a breach of data protection laws and could lead to large fines imposed by the Information Commissioner and/or civil claims being made against the business.

The intention of this policy therefore is to establish rules that define how information must be handled when it is left unattended.

Details of the policy

- When not being used, confidential information and personal data held in hard copy form such as paper records must be stored out of sight in locked cabinets, drawers or other suitable office furniture.
- Information containing personal data or other confidential information must be stored away in locked cabinets, drawers or other suitable office furniture when not required and especially when work stations or desks are left unattended.
- All portable data storage and computing devices (e.g. USB sticks, CDs, DVDs, tablets and phones) which contain confidential information must be stored in a locked location when not in use.
- When leaving a computer for any period of time the screen must be locked to prevent unauthorised viewing or access to information on the device. Screens will be configured so that they automatically lock if no activity takes place for a period of 7 continuous minutes.
- Any material that is printed must not be left unattended on printers or at any other locations. Where a print job has been started, the user must wait at the printer for this to complete and remove all printed pages relating to that job before they leave the area.
- If confidential information is found unattended in any location it must be immediately secured.
- Personal data and confidential information must not be displayed in any public place including when on public transport. Displaying personal data or confidential information on a laptop screen – if working in a public area including when on public transport – is acceptable with the use of a "privacy screen".

Further Guidance

- Securely put away completed files as soon as you have finished using them.
- Use secure recycling bins for office paper that you no longer need and never dispose of confidential information/personal data in general waste bins.
- During the course of relocation events such as office moves etc, always ensure that documents and equipment are moved safely and securely and that documents containing personal data or confidential information are never disposed of in general waste bins or left in any place where they could be seen by unauthorised persons, stolen or copied.
- Always adhere to the Data Retention and Destruction Policy when disposing of personal data or confidential information.
- Do not print emails or other documents unless necessary.
- Review the items on and around your desk to ensure you need them.
- Always clear your working area before you leave the office.
- Where possible, scan paper items and file them electronically on SharePoint or your appropriate system.

10. Password Strength Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must use a strong password that adheres to the guidance below**
- **You must never disclose your password to another person**
- **You must not write your password down and leave it on display or where it could easily be found**

Introduction

This policy describes how you should select your password for access to work network and IT systems and how often you must change your existing password. The purpose of this policy is to reduce the threat of a security incident that could lead to the accidental or unlawful loss, destruction, alteration, unauthorised disclosure or access to personal data or other confidential information transmitted, stored or otherwise processed.

Data protection laws require us to, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. We must therefore use appropriate technical and organisational measures to restrict access to our network information and other IT systems. Setting a strong password and changing it regularly is likely to reduce the risk of a security incident occurring.

Details of the policy

When selecting a new password or changing your existing password, always ensure that you:

- Use no less than 10 characters.
- Include the use of special characters such as symbols.
- Include a mixture of lower and upper case letters.
- Use a mixture of alphabetical and numerical characters.
- Change your password every 2 months and never use the same password more than once.
- Do not use common or weak passwords e.g. "123456" or "password" etc.
- Do not use passwords that are easy for others to guess.
- Never tell anyone else your password.
- Never write your password down and leave it on display or anywhere else where someone could easily find it. Always try to memorise your password or use a secure password authentication system.

11. Email & Digital Message Protection Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

1. **All electronic messages containing personal data or other confidential information must wherever possible only be transmitted via a Group IT authorised system and no other;**
2. **Personal data and confidential information must not be transmitted unless we have a lawful basis for doing so and where there is a clear business need;**
3. **Special category data must NOT be transmitted unless a clear exemption applies and unless the processing has been pre-authorised by Group HR and / or Legal;**
4. **The recipient of the data must be known to the business;**
5. **Where personal data is to be transferred to a destination outside the EEA, you must obtain prior written authorisation from Group HR and / or Legal and implement the safeguards which Group HR and / or Legal directs you to use for the transfer.**

Introduction

This policy describes how personal data is to be transmitted when it is sent both within and outside the organisation. It also describes the additional measures that must be taken when personal data is transmitted to destinations in countries outside the European Economic Area (EEA). In order to ensure that personal data is not processed unlawfully when it is transferred outside the EEA, you should seek prior authorisation from Group HR and / or Legal before it is transmitted. Group HR and / or Legal will check that the appropriate safeguards are in place for the personal data to be transferred internationally. Seek advice from your manager if you are in any doubt as to whether processing personal data involves transferring the data outside of the EEA.

Special Categories of Personal Data

Remember that personal data cannot be processed at all unless we have a lawful basis for processing it. In addition, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is **prohibited** unless certain exemptions apply. Such data is known as "special category data" because it is particularly sensitive personal data. The exemptions are contained within Article 9 of the GDPR and are as follows:

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes (except where the law provides that the prohibition on processing special category data cannot be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in the GDPR;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

You should seek advice from Group HR and / or Legal if you are in any doubt as to whether personal data that might be processed constitutes special category data.

Details of this policy

6. All electronic messages containing personal data or other confidential information must wherever possible only be transmitted via a Group IT authorised system;
7. Where it is not possible to utilise Group IT authorised system, we will notify all staff of what alternative arrangements are to be used including what additional security measures must be put in place when transmitting personal data;
8. Personal data and confidential information must not be transmitted unless we have a lawful basis for doing so and where there is a clear business need;
9. Special category data must NOT be transmitted unless a clear exemption (above) applies and unless the processing has been pre-authorised by Group HR and / or Legal;
10. The recipient of the data must be known to the business;

Where personal data is to be transferred to a destination outside the EEA, you must obtain prior written authorisation from Group HR and / or Legal and implement the safeguards which Group HR and / or Legal directs you to use for the transfer.

12. Bring Your Own Device Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must register a BYOD device with IT before using it for work purposes**
- **You must not use business IT networks for personal web browsing or video streaming**
- **You must adhere to the security standards and conditions of use detailed below**

Introduction

Employees are permitted to use their own smartphones, tablets and laptops at work for their convenience should they wish to do so, however, we reserve the right to revoke this privilege if users do not abide by the contents of this policy. This practise is referred to as "Bring Your Own Device" or "BYOD". The policy is intended to allow employees the option of using their own devices for work purposes should they wish to do so but also to protect the security of our network and IT systems in such circumstances. It sets out what constitutes acceptable use, the minimum security requirements which must be implemented on employee devices and other conditions of use.

Acceptable use

Only devices which have been registered as BYOD by IT will be permitted connectivity to the business IT networks. Use of the business IT networks are for business purposes only. The business IT networks must not be used for personal web browsing or video streaming etc. Devices must be presented to IT for proper configuration prior to being used for work purposes. Please note that employees will NOT be reimbursed for the cost of the device or for their use of their device or network for work purposes.

Security Standards and conditions of use

- Access requirements for the device must adhere to the password strength policy.
- The device must lock itself with a password or PIN if left unused for one continuous minute.
- After ten failed login attempts, the device should automatically lock.
- It is prohibited to use a device where the device itself or the operating system it uses have been significantly modified by any party other than the original manufacturer.
- All software updates and "patches" must be implemented as soon as reasonably possible after having been made available by the manufacturer/operator.
- Smartphones and tablets belonging to employees that are for personal use only are not permitted to connect to the business IT networks i.e. connection with the network must only occur where use is intended for business purposes.
- The employee's device may be remotely erased by us if the device is lost, if the user's employment ends or if IT detects a problem that could lead to personal data being compromised e.g. in the event that the device becomes infected by a virus or similar threat that could adversely affect the business. Please note that this means you should back up your personal content off the phone should the need ever arise to remotely wipe your device – it could mean all your photos etc are lost if they are not backed up.
- We may disconnect devices or disable services at any time at our discretion.
- Lost or stolen devices must be reported to the business by the employee within 2 hours of discovering the theft/loss.
- The employee is personally liable for all costs associated with their device.
- The employee accepts that they use their own device for work purposes at their own risk. The business will not be liable for any loss or damage caused to the employee's device as a result of the employee's use of the device for work purposes.

The business reserves the right to take disciplinary action for non-compliance with this policy.

13. Penetration Testing Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must at all times remain vigilant to cyber-security threats posed to the business**
- **You must adhere to all business policies and procedures relating to the protection of personal data and the security our physical premises and IT systems**
- **If in doubt about any security related issues, you should seek immediate guidance from Group HR and / or Legal**

Introduction

The security and integrity of our network and information systems is critical to the success of the business. It is also an essential part of our compliance with data protection laws such as the General Data Protection Regulation (GDPR). Although we operate a policy and procedure for dealing with a data breach event and similar security threats, it is equally important for us to remain vigilant and alert to risks. Cyber security threats adversely affect businesses across the world and new, more sophisticated digital threats such as viruses, malware and spyware are being developed by hackers and criminals every day. It is vital that we implement reasonable technical and organisational measures to protect the data – including personal data – which we hold so that we can comply with our legal obligations and continue operating successfully. A cyber-attack has the potential to significantly disrupt the business by preventing us from operating (due to system down-time or damage to our hardware). It could also result in other costs such as ransom payments, fines from the ICO, damages awards (and other legal costs) as well as reputational damage.

What we must do

In order to tackle this threat, all staff are expected to comply with all policies and procedures relating to security and the protection of data. In addition, we will undertake regular testing of our network and information systems. We will conduct the following exercises on a regular basis and record and analyse the results in order to assess potential vulnerabilities and enhance our security:

1. Network penetration testing by a reputable external IT company
2. Regular testing of our physical security at our office premises
3. Spot checks to ensure compliance with data protection policies
4. Regular system checks/audits

Results of all testing and spot checks will be analysed by the board in order to assess compliance and improve standards where necessary.

1. Network penetration testing by a reputable external IT company
   To take place at least once a year.
2. Regular testing of our physical security at our office premises
   To take place at least once a year.
3. Spot checks to ensure compliance with data protection policies
   To take place randomly at least four times per year
4. Regular system checks/audits
5. To take place randomly at least once per year

14. Physical Security Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must not allow unauthorised persons access to business premises at any time**
- **You must immediately notify management in the event that an unauthorised person gains access to business premises or where you suspect that this is the case**
- **You must adhere to the company's policies regarding the protection of hard copy data and information assets**

Introduction

The security of our physical assets is an important part of keeping our employees and staff safe as well as in ensuring the protection of personal data. This policy details the physical security arrangements that must be maintained at our premises as well as steps that all members of staff are expected to take in order to ensure the security our premises and physical assets such as smart phones, laptops and manual information which may all contain personal data controlled by the company.

Protection of premises

- Staff will only be permitted entry to company, or where we control, site premises with with a valid ID card.
- All members of staff must ensure that they do not allow unauthoried persons access to the company's premises.
- Staff should immediately notify management in the event that an unauthorised person gains access to company premises or where it is suspected that an unauthorised person has gained access, is attempting to gain access or has tried to gain access to the building.
- All visitors to the company's premises must sign in at reception and carry a visitor pass at all times during their visit.

Protection of hard copy personal data

- When not being used, any documentation, records, files or any other form of hardcopy information including personal data must be stored away in secure storage such as filing cabinets, drawers and other appropriate office furniture provided for by the company.

- All such items of office furniture must be locked when unattended. When leaving the office for the day or otherwise when leaving your desk or working area for any period of time exceeding five minutes, staff must ensure that all documentation is stored securely as per the above.

- Company owned devices such as laptops, smart phones and tablets should also be locked away when not in use. Devices should not be left on desks overnight or for any significant period of time.

- Staff are not permitted to make copies of original documentation unless authorised in writing by Group HR and / or Legal. Furthermore, staff are not permitted to remove documentation owned by the company from the company's premises unless directly authorised by management to do so for a clear business reason.

Registers

The company will operate appropriate registers to document the following:

i. Information assets
ii. Personal data processing activities
iii. Staff training records
iv. Records pertaining to the annual reviews of the following systems
    a. Registers
    b. Policies and procedures
    c. Physical security
    d. Network and information system security reviews
    e. Spots check relation to policy compliance
    f. System checks
v. Use of Processors/Sub processors
vi. Personal data breaches
vii. Near miss data security incidents
viii. Data Subject Rights requests

Registers will be reviewed at least once per year in order to assess performance, patterns/trends and to determine whether any action is necessary in order to address any issues identified by the review or otherwise improve security measures.

15. Staff Training (Data Protection) Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings. We have created a dedicated training platform, Advantage, that contains 4 training modules on data security and protection.
All staff must complete these modules on Advantage within 2 months of starting with the Group.

Key points to remember

- **You must ensure that you attend all training sessions arranged by the business and adhere to the rules and guidance provided during the training sessions**
- **You should direct any queries that you have about data protection matters or the training sessions provided to Group HR and / or Legal**

Introduction

Staff training is a key factor in the protection of personal data and in ensuring compliance with data protection laws. All staff will receive training on data protection matters, the General Data Protection Regulation and the company's policies and procedures relating to data protection and security. All training provided will be reviewed annually in order to ensure that content remains suitable and appropriate to the current law and the company's standards.

Training provided

The following data protection training will be provided:

a. To all new staff on induction
b. Refresher training to all staff to take place annually
c. Updater training to take place as when required following significant developments to data protection law and/or company policy and procedure concerning data protection.

16. Disaster/Incident Recovery Policy & Procedure

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **You must familiarise yourself with the company's Disaster/Incident Recovery Policy**
- **You must ensure that you adhere to the Disaster/Incident Recovery Policy in the event that the policy is invoked**
- **You should direct any queries relating to the policy to Group HR and / or Legal**

The company operates a Disaster/Incident Recovery Policy which sets out a procedure to follow so that the business is able to recover from and resume/continue operating following a major incident such as a natural disaster.

The policy can be obtained from either Group IT or Group Legal.

17. Data Retention and Destruction Policy

All members of staff must familiarise themselves with the contents of this policy and ensure that they adhere to the policy at all times. Failure to adhere to this policy may result in disciplinary proceedings.

Key points to remember

- **In most cases, personal data cannot be held by the business indefinitely**
- **This policy determines for how long personal data must be held**
- **When this policy has determined that personal data is no longer required, it must only be disposed of in accordance with this policy**
- **The business will determine the appropriate retention period for data – as detailed within our Data Audit Matrix**
- **The IT department will be responsible for the secure destruction of data held in digital form**
- **Personal data and confidential information must only be disposed of using the confidential waste bins provided and must NEVER be placed in general waste bins**
- **Only authorised personnel are permitted to destroy personal data**

Introduction

In order to comply with our obligations under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, the company must operate an appropriate policy and procedure for ensuring that personal data we hold is only retained for as long as we need it and that, once personal data is no longer required, it is safely and securely erased/destroyed so that it can no longer be used.

The GDPR requires us to process personal data in accordance with the Principles relating to the processing of personal data. These Principles are that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4. 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 ('accuracy');

5. 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; ('storage limitation');

6. 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 ('integrity and confidentiality').

In order to comply with these Principles and, in particular, the **'storage limitation'** and **'integrity and confidentiality'** Principles, it is crucial that we do not retain personal data for longer than necessary. In addition, the GDPR Accountability Principle means that we are responsible for and must be able to demonstrate our compliance.

The period of time between collecting a data subject's personal data and permanently erasing it is known as the "retention period". The retention period for personal data will vary depending on the nature of the personal data in question and how long we need to keep it. The company operates a Data Audit Matrix which records the categories of personal data held and specifies the period for which it must be retained.

Secure destruction of physical personal data

The company uses the services of an external company to regularly collect and securely shred confidential waste. All confidential hard copy, paper documentation and documentation containing personal data should be disposed of in the confidential waste bins provided by the company and located around the company's offices. Confidential information and personal data should NEVER be disposed of in regular waste or recycling bins or skips or placed elsewhere other than a confidential waste bin once it is no longer required. Confidential waste bins will then be emptied regularly by a nominated member of staff or employees of the external company with whom the company contracts to remove and securely shred the contents of confidential waste bins. If any member of staff sees confidential material and/or personal data left unattended or placed in general waste bins, they should report it immediately to their line manager.

Secure destruction of digital personal data

The IT department is responsible for the secure destruction of digital personal data stored on the company's servers and will take steps to permanently delete data stored on our servers in accordance with periods set out above. The IT department will also be responsible for the secure and safe destruction of IT hardware that has reached the end of its life. Devices should be handed back to the IT department when they are no longer to be used.

Signed:  Phil Munnelly, CEO