Gail Khan Associates

GDPR Policy

Created By:	Melanie Thompson
Approved By:	Gail Khan
Version:	1.1
Created on:	20 January 2020
Amended on:	24 January 2020
Next review date:	January 2021

Introduction

As a business we collect, process and hold personal information from our Clients and Colleagues on a daily basis, as such we are classed as a data processor under the Data Protection Act 1998 (DPA), to be superseded by the General Data Protection Regulations 2018 (GDPR), and it is a requirement that we are registered with the Information Commissioners Office (ICO).

The processing of personal data is governed by the GDPR and more specifically in connection with electronic marketing by the Privacy and Electronic Communications Regulations (PECR).

As a business we must take sufficient measures to ensure personal data is obtained for legitimate purposes and is adequate, relevant and not excessive for those required purposes. This data must be accurate and kept up to date and should not be kept longer than is necessary to fulfil its purpose. We also need to take measures against unauthorised and unlawful processing, loss, destruction or damage of the personal data held. The purpose of this policy is to ensure you do not breach the Regulations. **If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from Gail Khan, Director of Gail Khan Associates.**

Policy

It is our Policy to only collect and retain data that is reasonably necessary for the Company to conduct its legitimate business interests, to respect the privacy of individuals and to ensure that any data held is secure, treated as confidential, and protected against unauthorised access. This applies to both manual and computerised data.

Responsibility

Everyone within Gail Khan Associates has a responsibility to adhere to the rules of the Data Security Policy. Everyone has key responsibilities for the implementation, application and monitoring of this policy. You should be aware that you could be criminally liable if you knowingly or recklessly disclose personal data in breach of the Regulations. A serious breach of data protection is also a disciplinary offence and will be dealt with under the Company's disciplinary procedures. If you access another Colleague's personnel records without authority, this may constitute serious misconduct and could lead to your summary dismissal. Similarly, any Colleague that deliberately (or by reckless or negligent action) discloses personal information will also be considered to have committed serious misconduct.

Compliance with the Regulations is both the responsibility of the company and our individual Colleagues. In regards to the action of our colleagues, given below are the things that everyone should adhere to in the course of their daily duties:

- Colleagues must ensure that computer systems are not left unlocked while unattended.

- Passwords should be protected and changed on a regular basis.

- Documents detailing personal information should not be left unattended and should be securely stored when not in use.

- When communicating personal information, a secure form of media should be used that does not enable unauthorised persons to read it.

- Colleagues should not retain personal information about other colleagues or clients (or release it to a third party), without the express permission of Gail Khan and the person who is the subject of the information.

- Colleagues should be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone. If any doubt exists, authorisation from Gail Khan must always be gained before any information is released.

- Colleagues should ensure that any personal data you hold is kept securely, either in a locked filing cabinet or, if computerised, it is only held on authorised systems. Similarly, personal data must not be stored on mobile phones or other storage devices such as USB memory sticks.

How We Collect and Process Your Data

We will collect, hold and process client's personal data fairly and lawfully, in order to meet the legitimate business interests of the Company.

We will assess the business need and interest for each type of personal data we collect and hold. Personal data obtained and retained on individuals will be relevant and not excessive in relation to the purpose for which it is required. It will be accurate and kept up to date. Personal data shall not be transferred to a third party, unless it is necessary to meet a legitimate interest of the Company. Examples of such third parties include (but are not limited to) legal practices, multi-academy trusts and local authorities.

Appropriate technical and organisational measures shall be undertaken against unauthorised or unlawful processing of personal data, and to protect it against accidental loss, destruction or damage.

Personal data will only be accessed by authorised persons to carry out their designated duties within the business. In the case of data stored electronically this will be strictly controlled with appropriate security measures, both at an individual and organisational level.

All PC's, computers, phones and Laptops that may enable access to personal data should be logged off or locked when left unattended.

Training

We will provide suitable training to all new and existing colleagues to ensure that they are both aware and competent with the provisions of the Regulations on an ongoing basis.

It is your responsibility to meet and successfully complete these training requirements and in the case of ongoing training, to ensure that such training is completed in a timely manner. The expiry of training accreditation without good reason will be considered to be a serious disciplinary matter.

Prohibited Actions

Every colleague has the responsibility to comply with the requirements of this policy. This includes ensuring that you are careful and diligent with personal data and the systems we use to manage it. The failure to comply with this policy (or negligence when processing data) will be regarded as serious misconduct. Depending on the seriousness, this may also be regarded as gross misconduct and may result in summary dismissal. Individual criminal prosecution may also be appropriate. Examples of actions which are strictly prohibited and likely to be considered as gross misconduct are given below. This is not a definitive list: -

- The unauthorised access of Company systems or enabling a third party to make unauthorised access of Company systems.
- The unauthorised access to, damage of, copying of; or removal of Company documents and/or personal data (e.g. staff, customer, product information, or any other proprietary information). For the avoidance of doubt, this includes but is not limited to downloading, photographing, emailing, photocopying, posting on social media or the physical theft of documents or data.
- The unauthorised release of Company documents and/or personal data to a third party or persons.
- Serious negligence that causes (or is likely to cause) the loss of Company documents and/or personal data.

Sign Off

Approved By (print name):	Gail Khan
Role Title:	Managing Director
Signature:	
Date:	24 January 2020