DATA PROTECTION POLICY

Policy Statement

G&L Consultancy Ltd's data protection policy sets out the company's commitment to protecting personal data and how that commitment is implemented with regard to the collection and use of personal data.

G&L Consultancy Ltd is committed to:

- ensuring compliance with the six data protection principles of the Data Protection Act 2018 and the related seven key principles of the General Data Protection Regulations 2018;
- meeting legal obligations as laid down by the Data Protection Act 2018;
- meeting legal obligations as laid down by the General Data Protection Regulations 2018;
- ensuring that data is collected and used fairly and lawfully;
- ensuring data is used only for specified, explicit purposes (such as to meet operational needs or fulfil legal requirements);
- ensure data is only used in a way that is adequate, relevant and limited to only what is necessary;
- taking steps to ensure that personal data is up to date and accurate;
- establishing appropriate retention periods for personal data;
- ensuring that data subjects' rights can be appropriately exercised;
- provide adequate and appropriate security measures to protect personal data including protection against unlawful or unauthorised processing, access, loss, destruction or damage;
- ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues;
- ensuring that all staff are made aware of good practices in data protection;
- provide adequate training for all staff responsible for personal data;
- ensuring that everyone handling personal data knows where to find further guidance;
- ensuring that queries about data protection, internal and external to the organisation, are dealt with effectively and promptly;
- regularly reviewing data protection procedures and guidelines within the organisation.

Scope of Policy

This policy applies to all members of staff within G&L Consultancy Ltd. For the purposes of this policy, the term "Staff" means all members of staff including permanent, fixed term, and temporary staff, staff on secondment, any third-party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the company in the UK or overseas.

All contractors and agents acting for or on behalf of G&L Consultancy will be made aware of this policy.

For the purposes of this data protection policy, G&L Consultancy does not differentiate between the protection of personal data as prescribed by the Act and the protection of customers' confidential information and proprietary rights and the protection, electronic storage and transmission of results. Further information on this can be obtained within the relevant sections of G&L Consultancy Ltd's Quality Manual.

This document will also include the specific data protection policies G&L Consultancy Ltd has in place in relation to TEAMs (The Electronic Asbestos Management System) and its Client Portal.

Data Protection Principles

The Data Protection Act 2018 ('the Act') gives individuals the right to know what information is held about them and sets out legislative requirements for organisations processing personal data (referred to under the Act as 'Data Controllers'). The Act came into force on 25 May 2018.

The Act is the United Kingdom's implementation of the General Data Protection Regulation (GDPR) ("the Regulation").

The Act, the Regulation and the Freedom of Information Act 2000 are overseen and enforced by the Information Commissioners Office (ICO), which is an independent public body responsible directly to Parliament.

G&L Consultancy Ltd, as a data controller, will be open and transparent when processing and using personal information by following the six principles as set out in the Act and the related seven key principles set out in Article 5 of the Regulations, as listed previously:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 2018.
- Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Definitions

This policy applies to all personal and sensitive personal data processed and stored electronically and manually (paper-based) files. It aims to protect and promote the rights of individuals ("Data Subjects") and G&L Consultancy Ltd ("Company").

Personal Data

Any information which relates to a living individual who can be or may be identified from that information, for example:

- A person's name and address (postal and email)
- Date of birth
- Statement of fact
- Any expression or opinion communicated about an individual
- Minutes of meetings, reports
- Emails, file notes, handwritten notes, sticky notes
- CCTV / Dash Cam footage and / or photographs if an individual can be identified by the footage / images
- Employment applications
- Spreadsheets and / or databases with any list of people set up by code or staff number
- Employment history

Sensitive Personal Data

Any information relating to an individual's:

- Ethnicity
- Gender
- Religious or other beliefs
- Political opinions
- Membership in a trade union
- Sexual orientation
- Medical history
- Offences committed or alleged to have been committed by that individual

Data Subject

Any living individual who is the subject of personal data whether in a personal or business capacity

G&L Consultancy Ltd recognises and understands the consequences of failure to comply with the requirements of the Act may result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension / withdrawal of the right to process personal data by the Information Commissioners Office (ICO);
- Loss of confidence in the integrity of the Company's systems and procedures;
- Irreparable damage to the Company's reputation.

Where staff do not comply with this policy, the Company may also consider acting in accordance with the Company's established Disciplinary Procedure.

Staff Obligations

Staff will not gain access to information that is not necessary to hold, know or process. All information which is held will be relevant and accurate for the purpose for which it is required. The information will not be kept for longer than is necessary and will be kept secure at all times.

Staff will ensure that all personal or sensitive personal information is anonymised as part of any evaluation of assets and liability assessments except as required by law.

Staff who manage and process personal or sensitive personal information will ensure that it is kept secure and where necessary confidential. Sensitive personal information will only be processed in line with the provisions set out in this policy.

Staff are responsible for notifying their line manager or the Data Protection and Freedom of Information Manager if they believe or suspect that a conflict with this policy has occurred or may occur in the future. This includes notification of any actual or suspected data breach.

Company (Data Controller) Obligations

The Company will follow the Code of Practice issued by the ICO when developing policies and procedures in relation to data protection.

The Company will ensure that Data Processing and / or Sharing Agreements are applied to all contracts and management agreements where the Company is the data controller contracting out services and processing of personal data to third parties (data processors).

The Company will ensure this agreement clearly outlines the roles and responsibilities of both the data controller and the data processor.

The Company will adhere to and follow the principles of data protection and the Privacy & Electronic Communications (PEC) Regulations when conducting surveys, marketing activities etc and where the Company collects, processes, stores and records personal data.

The Company will not transfer or share personal information with countries outside of the European Economic Area (EEA) unless that country has a recognised adequate level of protection in place in line with the recommendations outlined in the Act.

The Company will ensure all staff are provided with data protection training and promote awareness of the Company's data protection and information security policies, procedures and processes.

Data Subjects Rights

The Company acknowledges individuals' (data subjects) rights under the Act to access any personal data held on our systems and in our files upon their request or to delete and / or correct this information if it is proven to be inaccurate, excessive or out of date.

The Company recognises that individuals have the right to make a request in writing to obtain a copy of their personal information if held on our systems and files.

The Company recognises that individuals have the right to prevent data processing where it is causing them damage or distress or to opt-out of automated decision-making and stop direct marketing.

The Company will only share information in accordance with the provisions set out in the Act and where applicable the Company will inform individuals of the identity of third parties to whom we may share, disclose or be required to pass on information to, whilst accounting for any exemptions which may apply under the Act.

CCTV / Dash Cam Specific Protection

CCTV footage (visual only) is stored on a secure server for a maximum of 3 months and only those persons with a valid username and password can access the footage. The recorded footage is not routinely monitored and is only accessed when required in the course of an investigation.

Dash Cam footage (audio and visual only) is stored on the onboard SD card. No images and information will be copied from the SD Card except where a relevant incident has occurred. Dash Cams only retain up to 30 seconds of the incident. However, it is possible to review up to 100 hours of video if deemed necessary during an investigation. The Dash Cams only record an external view through the vehicle's windscreen and cannot be accessed covertly to monitor employees.

The onboard SD card can be accessed via the Dash Cam however footage can only be copied / saved / viewed by those persons with a valid username and password for the Dash Cam Application. The footage is not routinely monitored and is only accessed when required in the course of an investigation.

TEAMs Client Portal Specific Protection

In addition to the protection offered under the Data Protection Act 2018 and described in this policy, G&L Consultancy Ltd has set out the following protection and information regarding TEAMs (The Electronic Asbestos Management System) Client Portal.

Portal Hosting Organisation

The TEAMs Client Portal is hosted by Mark One Consultants Ltd, Unit 5 - 6, Bartlett Court, Sea King Road, Lynx Trading Estate, Yeovil, Somerset, BA20 2NZ

Mark One Consultants also act in the capacity of both TEAMs software developers and online security consultants.

The TEAMs Client Portal is hosted on a secure server and is accessed through a secure gateway, denoted by the 'https' URL prefix and the image of a padlock in the address bar.

Mark One Consultants and G&L Consultancy Ltd are signatories to a separate non-disclosure and confidentially agreement which includes the TEAMs portal and servers.

The management system of Mark One Consultants have been assessed by The British Assessment Bureau and has been certified as meeting the requirements of BS EN ISO/IEC 27001:2017 (Certificate Number 212051).

Portal Log in Details

In order to gain access to the TEAMs Client Portal all users require a valid email address, username and password.

Different levels of access can be allocated to different users for the same client.

User access is achieved by the named client representative requesting access, in writing and including the following information:

- Name(s) of third party;
- Email address(es) of third party;
- Level of required access;
- Date access required from;
- Date access should be rescinded.

G&L Consultancy Ltd will then set up the correct level of access and provide an individually generated password which is emailed directly to the named user.

It remains the client's responsibility to ensure that user details and access levels required are kept current and up to date and that they notify G&L Consultancy Ltd if any access requires removal.

Authorised Third Party Access

Only those persons with a valid username and password can access the portal, this includes the employees of both G&L Consultancy Ltd and Mark One Consultants.

If third-party access is required as requested by a client, this request must be received in writing and include the following information:

- Name(s) of third party;
- Email address(es) of third party;
- Level of required access;
- Date access required from;
- Date access should be rescinded.

Unauthorised Third Party Access ("Hacking")

In the event of a malicious attack on the portal or an attempt to gain access by circumnavigating the built-in security protocols, Mark One Consultants have in their hosting capacity a number of security options available in order to deflect / defeat the attack / hack up to and including taking the portal in its entirety offline until the issue(s) have been identified and dealt with.

Downloading of Data

Data present on the TEAMs client portal can only be downloaded by an authorised user and only at the access level they have been granted.

The portal retains an audit trail of each action and this includes:

- Category of action
- User name
- Reference number
- IP address
- Time of action

Retention of Data

All data uploaded to the client portal by any party will be retained until such time as notice is received in writing from the client that the data is no longer required.

In the event that a client no longer wishes to use the services of G&L Consultancy Ltd but does require continued access to the portal, the access and all responsibility for the data stored on the portal will transfer to the client.

Complaints

Individuals who wish to make a complaint relating to breaches of the Data Protection Act 2018 and / or complaints that an individual's personal information is not being processed in line with this policy may do so in writing to:

Julie Lewis, Quality Director
G&L Consultancy Ltd
Unit 5A Chelston Business Park
Castle Road
Wellington
Somerset
TA21 9JQ

DATA PROTECTION POLICY

This policy has been endorsed by Julie Lewis and has the full support of the management team.

The policy was reviewed and approved on 16th January 2023 following consultation with senior managers and workers.

Overall responsibility for the effectiveness of the policy lies with Julie Lewis, Quality Director. For more information, please contact this person: 01823 443 898

Director	Name	Signature	Date
Quality Director	Julie Lewis	*Julie Lewis*	16th Jan 2023
Technical Director	Paul Lewis	*Paul Lewis*	16th Jan 2023
Somerset Office	**Name**	**Signature**	**Date**
Health, Safety and Quality Manager	Mark Skinner	*Mark Skinner*	16th Jan 2023
Operations Manager	Darren Alway	*Darren Alway*	16th Jan 2023
Client Liaison Manager	James Ooyman	*James Ooyman*	16th Jan 2023
Wages, Personnel and Accounts Manager	Sally Monger	*Sally Monger*	16th Jan 2023
Air Test & Removals Manager	Jason Monger	*Jason Monger*	16th Jan 2023
Survey Manager	Jo Haigh	*Jo Haigh*	16th Jan 2023
Northern Ireland Office	**Name**	**Signature**	**Date**
Northern Ireland Director	Alan Lewis	*Alan Lewis*	16th Jan 2023
Office Manager	Karen Lewis	*Karen Lewis*	16th Jan 2023
Lab Manager	Colin Webb	*Colin Webb*	16th Jan 2023
Deputy NI Branch Manager	John McAleenan	*John McAleenan*	16th Jan 2023