Data Protection Policy

Data Classification, Handling and Disposal

Tony Gee
Consulting Engineers

1. Purpose

This document sets out the company policy with respect to data protection. The purpose of this document is to define a system of categorising information in relation to its sensitivity and confidentiality, and to define associated rules for the handling of each category of information to ensure the appropriate level of security (in relation to confidentiality, integrity and availability) of that information.

The policy aims to:

- protect information from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence
- help to meet legal, ethical and statutory obligations
- protect the interests of all those who have dealings with the business and about whom it may hold information (including its employees, directors, clients and suppliers)
- promote good practice in relation to information handling.

The use of all personal data is governed by:

- The UK General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018 (DPA)
- The Privacy and Electronic Communications Regulations (PECR)

2. Scope

This policy covers all information held by and on behalf of Tony Gee and Partners LLP (Tony Gee) and the handling rules shall apply to members of the business and to third parties handling Tony Gee information. Where Tony Gee holds information on behalf of another organisation with its own information classification, agreement shall be reached where applicable as to which set of handling rules shall apply.

3. References

For information on how Tony Gee processes personal data in line with the GDPR please refer to the Privacy Notices available on the Tony Gee website. (Prospective, Current and Past Staff Members /Marketing and Business Operations)

This document should also be read in conjunction with the following documents

- PR-AD-009 – Archiving and Storage
- PR-AD-008 – Information and Communications Technology Services
- Computer Equipment and Internet Acceptable Use Policy
- Employee handbook

Data Protection Policy

Data Classification, Handling and Disposal

Tony Gee
Consulting Engineers

4. Policy Statement

All employees and directors of Tony Gee and third parties who handle information on behalf of Tony Gee have a personal responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling. We are committed to upholding the data protection principles as defined by the GDPR.

These require that all personal data be:

- processed in a lawful, fair and transparent manner.
- collected only for specific, explicit and limited purposes ('purpose limitation').
- adequate, relevant and not excessive ('data minimisation').
- accurate and kept up-to-date where necessary.
- kept for no longer than necessary ('retention').
- handled with appropriate security and confidentiality.

Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.

Automatic technical controls may be implemented to assist users in complying with these controls, but where technical measures are not implemented users are responsible for complying with this policy.

5. Policy

- All information held by or on behalf of Tony Gee is managed according to the Information Classification and Handling table in Appendix 1 unless additional measures are required by specific contract or client requirements. The categorisation shall be determined by the originator of the information. Where information falls within more than one category, the higher level of protection shall apply in each case.
- In accordance with UK legislation, information relating to employees, their payroll and employment record, training record, and personal contact information will be retained by Tony Gee for legitimate business purposes up to but not exceeding six years following termination of the employment contract.
- Where a third party will be responsible for handling information on behalf of Tony Gee, the third party shall be required by contract to adhere to this policy prior to the sharing of that information.
- Where Tony Gee holds information on behalf of another organisation with its own information classification, written agreement shall be reached as to which set of handling rules shall apply prior to the sharing of that information.
- We commit to upholding our registration to the Information Commissioner's Office Data Protection Register and will follow the practices published by them where appropriate.
- We will refer to the appropriate legislation regarding retention of medical records where necessary under UK legislation in particular in relation to COSHH and asbestos.
- We commit to maintaining adequate levels of cyber security and certification as required.

Data Protection Policy

Data Classification, Handling and Disposal

6. Responsibilities

The IT Director shall ensure that the Information Classification and associated Handling Rules are reviewed regularly to ensure they remain fit for purpose.

It shall be the responsibility of every individual handling information covered by this policy, to apply the appropriate handling rules to each category of information, and to seek clarification or advice from a director, or the Administration Manager where they are unsure as to how to label or handle information.

All employees and directors of Tony Gee shall report issues of concern in relation to the application of this policy, including alleged non-compliance, to the IT Director or Executive Managing Director.

7. Compliance

Breaches of this policy may be treated as a disciplinary matter, dealt with under Tony Gee's staff disciplinary policies. Where third parties are involved in the breach of this policy Tony Gee will follow the advice of the Information Commissioner's Office (ICO).

Signed:

C J Young

Executive Managing Director

Reviewed Date: January 2024

Data Protection Policy

Data Classification, Handling and Disposal

Tony Gee
Consulting Engineers

Appendix A – Information Classification and Handling

Category	Description	Examples	Storage location and protection	Dissemination and access	Disposal
Personal	Non-business information belonging to employees	Personal finance documents Correspondence related to home, family and friends	Private network folder provided which is backed up, however, any data stored elsewhere (e.g. desktop) will not be backed up.	Accessible by individual and IT system administrators.	Upon termination of employment HR informs IT and their folder is removed. No backup of personal data is kept.
Public	Business information that is specifically prepared and approved for public consumption.	Marketing materials and business announcements (e.g. gender pay), both online and in print. Corporate social media accounts. Openly available corporate governance information (e.g. Companies House).	Digital information should be stored using Tony Gee provided IT facilities and those of our website host, to ensure appropriate management, backup and access. Paper materials (brochures etc.) are held in stock either at our printer supplier warehouse or in our offices before being disseminated. Website host provides protection against vulnerabilities to potential hackers.	Published digital information can be accessed via the website without requiring a login or password. Website/social media author and editors must login and have a responsibility to choose a robust password and secure the login credentials appropriately. Electronic and hard copy information can be circulated freely subject to applicable laws e.g. copyright, contract, competition. This will be via email or postal services.	When no longer relevant. Publicly accessible online data will be removed. It may be archived for reference and ease of replication in future. Hard copy materials are recycled using normal office procedures.

Category	Description	Examples	Storage location and protection	Dissemination and access	Disposal
Restricted	Non-confidential information where dissemination is limited to direct contacts of Tony Gee, e.g. employees, clients, subconsultants, suppliers.	Company intranet, including controlled Management System policies and procedures (QMS, EMS H&S etc.) Business and premises administration documents and guidance notes. Internal databases for employee timesheets recording, project and client and supplier management. Non-confidential tender proposals. Project correspondence.	Generally accessible to all employees (when logged in) and backed up in accordance with Tony Gee IT security. Held on Tony Gee servers / cloud storage and protected accordingly.	To gain access to TG IT systems, users are provided with a login. All have a responsibility to choose a robust password and secure the login credentials appropriately. Data may be accessed remotely and via portable and mobile devices using Tony Gee IT security protocols.	The data retention period and archiving/destruction requirements will be defined in procedure PR-AD-009.

Category	Description	Examples	Storage location and protection	Dissemination and access	Disposal
Confidential	Information which is sensitive in some way because it might be personal data, commercially sensitive or legally privileged, or under embargo before being released at a particular time. This data has the potential to cause a negative impact on the interests of individuals or the company, if disclosed inappropriately.	Data and information held on employees or Directors whilst in the service of Tony Gee. Data limited to access by specific employees and line managers (e.g. annual appraisals). Benefits application forms and correspondence. Commercially sensitive documents such as Board meeting reports, minutes and financial performance. Confidential tender bids prior to award of contract which have specific non-disclosure or security agreements. Commercially sensitive projects as defined by Client contract. High level strategy documents. Government reporting and HMRC / ONS. CCTV footage from security cameras at certain premises.	This information requires tight security measures, controlled and limited access and protection from corruption. Strict permissions are set in relation to legitimacy of need for access and controlled accordingly. Personnel data stored on Tony Gee database with restricted permissions to key/senior team members and, upon request, the individual to which the data pertains. All commercially sensitive and personnel documentation are stored digitally on the Tony Gee network in a restricted access folder, using strict permissions. CCTV footage is stored by the landlord and not on Tony Gee premises. Data should not typically be stored on portable devices, laptops or storage drives (USB sticks etc) unless encrypted or password protected.	To gain access to TG IT systems, users are provided with a login. All have a responsibility to choose a robust password and secure the login credentials appropriately. Data may be accessed remotely and via portable and mobile devices using Tony Gee IT security protocols. To gain access to the restricted folders, users must have been granted specific permissions by senior leadership. Benefits correspondence is handled via secured email/external cloud-based portal systems with appropriate login security.	In accordance with UK legislation, following termination of employment through whatever means, records will be retained both on our database and in a folder structure for a period of six years. All personnel correspondence is digital, with hard copies being scanned immediately and the originals destroyed securely. Documents which are determined by law to remain as hard copy with wet-signatures etc. are held securely in accordance with contract requirements. For all other data, the retention period and archiving/destruction requirements will be defined in procedure PR-AD-009.

Category	Description	Examples	Storage location and protection	Dissemination and access	Disposal
Highly Confidential	Has the potential to cause serious damage or distress to individuals or serious damage to the company's interests if disclosed inappropriately.	Personal employment details including salary, discipline, sickness records etc. Highly commercially sensitive projects as defined by Client contract. LLP Governance documents including financial arrangements. Service Level Agreements for key suppliers.	This information requires significant security measures, controlled and limited access and protection from corruption. Strict permissions are set in relation to legitimacy of need for access and controlled accordingly. Personnel data stored on Tony Gee database with restricted permissions to key/senior team members and, upon request, the individual to which the data pertains. All commercially sensitive and personnel documentation are stored digitally on the Tony Gee network in a restricted access folder, using strict permissions. Data is not to be stored on portable devices, laptops or storage drives (USB sticks etc).	To gain access to TG IT systems, users are provided with a login. All have a responsibility to choose a robust password and secure the login credentials appropriately. Data may be accessed remotely and via portable and mobile devices using Tony Gee IT security protocols. To gain access to the restricted folders, users must have been granted specific permissions by senior leadership.	Documents which are determined by law to remain as hard copy with wet-signatures etc. are held securely in accordance with contract requirements. Upon receipt of hard-copy signed terms and conditions from new employees, the original is scanned and destroyed using an accredited confidential-waste supplier. For all other data, the retention period and archiving/destruction requirements will be defined in procedure PR-AD-009.