Information Security and Acceptable use Policies

Contents

1. Computer Equipment & Internet Acceptable Use Policy 2
2. Cyber Security Policy 4
3. Data Protection Policy 6
4. Data Management Policy 7
5. Artificial Intelligence (AI) Acceptable Use Policy 8

1. Computer Equipment & Internet Acceptable Use Policy

Purpose

This Policy sets out the company requirements with respect to acceptable use of company provided computers and related equipment, services and facilities.

General Policy

Tony Gee and Partners provides all staff with access to company computer and telecoms hardware, services (both on-premises and cloud-hosted), networks and connections to external networks (including the internet and mobile telephony networks) (all collectively, 'systems'). These systems are provided to assist staff in the performance of their jobs. All users have a responsibility to use Tony Gee's systems and resources in a professional, lawful and ethical manner. Abuse of the systems, or failure to comply with this policy, may result in disciplinary action, including possible dismissal.

- Permitted Personal Use: Limited appropriate personal use of the systems is permitted if such use does not a) interfere with any employee's job performance; b) have an undue effect on the computer or company's system's performance; or c) violate this or any other policies or guidelines of the company.
- Prohibited Uses: Tony Gee's systems may not be used to obtain, create, store or disseminate material that is inappropriate or unlawful. Such material includes (but is not limited to) text or images which may be considered obscene, intimidating, political, fraudulent, harassing, embarrassing, defamatory, discriminatory or infringe on any person's rights to privacy.
- Employees may not use Tony Gee's systems to play games or run entertainment software (including animated jokes). Connections may not be used to download games or other entertainment.
- Illegal Copying: Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to any material you wish to download or copy.
- Communication of Trade Secrets: Unless expressly authorised to do so, users are prohibited from using the systems to distribute or transmit proprietary or confidential information belonging to Tony Gee or its clients.
- Accessing the Internet: To ensure security and avoid the spread of viruses, users accessing the internet (or other external network) through Tony Gee's systems must do so through a method implemented by the computer department. Bypassing Tony Gee's computer network security by accessing the internet directly by any means is strictly prohibited.
- Frivolous Use: Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others.

- Virus Detection: Files obtained from sources outside the company, including on storage hardware (e.g. USB sticks) from home, files downloaded from the internet, files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the company's systems. All such material must be scanned with Tony Gee-approved virus checking software. If you suspect that a virus has been introduced into Tony Gee's systems, notify the IT department immediately.
- Waiver of Privacy Rights: All employees expressly waive any right of privacy in anything they create, store, send or receive using the company's systems or transmit on company provided connections. The user consents to allow company personnel access to and review of all materials created, stored, sent or received by the user through any company system or connection.
- Monitoring of System and Connection Usage: The company maintains the right to monitor and log any and all aspects of its systems including, but not limited to, monitoring internet sites visited by users, monitoring file uploads and downloads, and monitoring all aspects of communications sent and received by users via the systems or connections.

2. Cyber Security Policy

This Policy establishes the framework for protecting the digital assets, data, and information systems of Tony Gee. This policy applies to all employees, contractors, and third-party users who access the Company's IT systems. It covers all information assets, including data, software, systems, networks, and both fixed and portable devices.

All users with access to company information assets shall comply with the following measures, with the requirements of the company Data Protection Policy, and with the company Computer Equipment and Internet Acceptable use Policy:

Access Control

- User accounts shall only be assigned based on role-based access control (RBAC) and permissions reviewed when roles change and removed for inactive or leaving employees.
- Multi-factor authentication (MFA) shall be adopted wherever possible.
- Passwords and MFA secrets or codes must meet complexity requirements, must be unique to each individual and must never be shared.

Data Protection

- The company shall appoint a Data Protection Lead to advice the organisation regarding data protection law and data privacy matters, to monitor compliance, and liaise with regulators as required.
- All personnel handling data shall comply with the requirements of the Data Protection Policy and uphold the principles of the UK GDPR.
- Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.
- Company data shall not be stored on or transmitted by unapproved devices or systems (e.g. transmitted to personal email addresses).

Network System and Device Security

- The company shall implement firewalls and endpoint security solutions and users must not attempt to circumvent such systems.
- All software and hardware shall be updated regularly ensuring that vulnerabilities are addressed promptly, effectively preventing exploitation of known security issues. Patches for critical vulnerabilities shall be applied as soon as possible upon release.
- All remote connections to company internal systems shall be only from company-owned hardware with up-to-date endpoint protection, and all such connections shall use authorised VPN systems and be validated by MFA.
- Staff working from home shall comply with the security requirements of the ‘Home Working’ procedure.
- Staff shall not leave devices unattended in any public place.

Asset Management

- The company shall maintain an inventory of IT assets, including hardware and software.
- Unused or outdated assets shall be securely decommissioned and disposed of, including by physical destruction of data storage media.

Incident Response and Reporting

- All security incidents must be reported to IT immediately.
- Any incident that may constitute a data breach shall be reported to the company IT Director and Data Protection Lead for assessment and possible reporting to the ICO.

Training and Awareness

- The company shall carry out periodic cybersecurity awareness training and all staff shall complete mandated training promptly.
- The company may carry out covert testing of staff cyber security awareness (e.g. phishing campaigns) and staff shall cooperate with these tests.

Business Continuity and Disaster Recovery

- The company shall complete regular data backups which will be stored securely and tested for recovery periodically.
- A documented Business Continuity Plan shall be maintained.

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.

Elements of this policy may be delegated to contractors or suppliers, but where this is done a written contract or statement of work shall be agreed defining responsibility for any elements of this policy so delegated.

3. Data Protection Policy

All Personnel 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. Tony Gee is committed to upholding the data protection principles as defined by the UK GDPR.

Tony Gee adheres to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency);
- collected only for specified, explicit and legitimate purposes (purpose limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);
- accurate and where necessary kept up to date (accuracy);
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);
- not transferred to another country without appropriate safeguards in place (transfer limitation); and
- made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (data subject's rights and requests).

Tony Gee is responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability).

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.

4. Data Management Policy

Tony Gee and Partners LLP provide specialist civil, structural and geotechnical design services to the construction industry. This policy outlines how project data including geotechnical, CAD/BIM data, monitoring and client provided data is managed throughout its lifecycle.

Tony Gee is committed to:

- Continuously improving our data management systems.
- Protecting data, in accordance with our Data Protection Policy, GDPR and client requirements.
- Respecting client, intellectual property and third-party data usage rights.
- Managing geotechnical data in accordance with BS 8574 in the UK and other relevant National Standards.
- Applying secure data handling practices, including encryption and access controls, aligned with industry standards to protect project and client data from cyber threats.
- Managing change control, transparent across all data lifecycle stages (receipt, validation, storage, use, archiving and disposal)
- Validating data appropriately for its intended use and associated risks.
- Training our staff in effective data management.
- Adhering to defined data retention periods (see PR-AD-009 Archiving and Storage).

We will implement this policy by:

- Appointing a 'Data Manager' for projects, this shall be the Project Engineer by default unless assigned to another individual.
- Ensuring secure data collection and storage with appropriate project specific security controls.
- Defining roles and responsibilities of staff in handling of geotechnical data.
- Maintain traceability and transparency in data source, change control management, error management.
- Using repeatable, auditable methods for data verification and validation.
- Apply consistent framework for data creation, processing and interpretation.
- Producing drawings and figures aligned with our QMS procedures.
- Manage commercial risks in data import/export for Tony Gee deliverables.
- Develop coordinated geometric and enriched data models for use by other design teams and disciplines.
- Implementing version control and data management in Common Data Environments e.g. ProjectWise, Autodesk Construction Cloud.

The Management of Tony Gee are committed the implementation of this policy and ensure adequate training and resources are made available to do so. It is every employee responsibility to co-operate fully in the implementation of this policy. This policy is reviewed annually to ensure it remains effective and relevant to any changing facets of the industry.

5. Artificial Intelligence (AI) Acceptable Use Policy

Purpose

This Policy sets out the company requirements with respect to the use of Artificial Intelligence (AI) based technology within Tony Gee and Partners LLP (Tony Gee).

We want to adopt a pro-active approach to AI within Tony Gee, maximising the potential of AI based tools and process, balanced with an appropriate level of risk management and ability to adapt in a fast-moving technology environment, to ensure that Tony Gee remains competitive in our relevant markets.

The policy aims to.

- Allow appropriate, safe and ethical use of AI based tools within Tony Gee
- Protect our colleagues and business from risks including.
    - Compromise of our systems, data and intellectual property (IP)
    - Potential legal liabilities arising from the use of AI generated content, or as a result of the compromise of our systems.

Regulatory requirements and best practice related to the use of AI tools are developing and unclear. We anticipate these may develop rapidly and vary by region, and client expectations and contractual requirements are starting to adapt to incorporate AI. Therefore, this policy will be reviewed by the Digital Steering Group (DSG) at least every 6 months to ensure that our approach and controls remain appropriate.

Scope

This policy applies to.

- All staff, contractors or 3rd parties who have a business need to operate and use IT systems within Tony Gee.
- Any automated system or process that may make use of AI based technology.
- Internal AI: Tools either created by Tony Gee or purchased by Tony Gee that utilise data not visible outside of Tony Gee.
- External AI: Tools available directly from the internet or unmanaged 3rd party providers, including.
    - Dedicated AI tools, for example ChatGPT, Microsoft Co-Pilot, Google Gemini
    - Vendor provided AI tools, for example tools built into our key software tools (Microsoft, Autodesk, Bentley, Adobe etc.)

References

This document should be read in conjunction with the following.

- Data protection policy
- Computer Equipment and Internet Acceptable Use policy
- PR-AD-008-18 Information and Communications Technology Services
- All policies, procedures and guidelines related to the production and quality assurance of information produce by Tony Gee.

General Policy

All employees and directors of Tony Gee, and 3rd parties working with Tony Gee systems and information have a responsibility to ensure that AI is used safely and responsibly.

Tony Gee will ensure adequate training and support is provided to all employees to allow AI to be used safely and responsibly.

Most of the Artificial Intelligence use within Tony Gee would be considered as Generative AI – i.e. the AI tools are used to generate some form of output which could be used as content in our production information or used as basis to inform decisions. Users should always ensure that AI generated content is subject to appropriate review, as outlined below, before being used elsewhere.

AI generated content should not be used to determine an action in an automated process, nor should it be further re-used in any automated process without human intervention. For example, many of the automation tools we have access to (Power Automate, Dynamo, Grasshopper etc.) have the capability to access AI services as part of the workflow to both submit and retrieve information. Any workflow developed with these tools should ensure that the process cannot continue without human intervention when AI content is created.

In all cases, if in doubt, do not use the AI tool or content generated by AI. Refer to the DSG for further advice and guidance.

No system or process involving AI, either business process, or project/design applications, should be developed within Tony Gee without the notification, and/or involvement of, the DSG.

AI Specific Risks

Whilst the use of AI presents several benefits and opportunities, it also presents a number of risks which we need to consider. Many of which are unique to the use of AI and therefore have not been a consideration in our use of technology before.

Careful consideration of the risk associated with the application of AI is required and will vary depending on the application.

Some of these risk factors also need to be taken into consideration when checking and using information produced with the aid of AI.

The following risks documented here are provided for guidance, however, are not comprehensive. Each application of AI should consider AI risks within the context of the application.

If in doubt liaise with the DSG before using an AI application.

Reliability

- Accuracy and correctness: AI may produce results that are not factually correct, or not logical or not sensible.
- Reproducibility: Assessing the accuracy and reliability of outputs from AI may be difficult or impossible, as models can produce different outputs in response to the same prompts.
- Fairness: Biases in data or design may be introduced consciously or unconsciously and may result in unfair or misleading results.

- Explainability: Valid decisions should be supported by explainable justifications for discussion or audit purposes. Generative AI replies may provide answers which are not readily explainable.

Compliance

- Personal data protection: Risks related to individual privacy may emerge if users enter details that later appear in the AI's generated content in a way that reveals their identity. Additionally, generative AI technologies have the potential to produce and spread harmful content like misleading information, manipulated videos, and hate speech.
- Intellectual asset concerns**:** The use of training data and the resulting outputs from generative AI carry substantial risks related to intellectual property, such as violations of copyright, trademark, patent, or other legal protections. Organisations employing generative AI services must be aware of the data sources used for training and how that data is manifested in the generated content.
- Cybersecurity: Malicious actors could potentially exploit generative AI to enhance the efficiency and complexity of cybercrimes. These AI models are also susceptible to tampering that produces harmful outputs. Organisations must safeguard key data (e.g. passwords) to ensure these are not shared with AI that may then misuse them.

Impact

- Liability: The organisation may be subject to legal and regulatory liability, and may damage customer, partner, supplier, or other stakeholder relationships. It may not be clear whether providers of AI can be held liable for the outputs of their own software.
- Organisational impact: The internal workforce or local communities or other groups could be negatively affected.
- Social and environmental impact: There may be detrimental social and environmental consequences, perhaps far more serious than could have been anticipated.

Acceptable use of AI

AI Tools

The general approach to the use of AI tools within Tony Gee will be to maintain visibility of tools in use, and specifically identify tools which should not be used.

The use of new AI tools should be identified and the DSG notified prior to use.

The DSG will maintain and publish a register of AI tools in use within Tony Gee. This register will include any specific considerations required regarding its use.

Data Management

Consideration should be given to the origin of data used in Generative AI processes and data provided to AI tools during their use.

Many AI systems will use any data provided to the system to further train the systems model, meaning that this data could be provided to other users of the system as part of a response to a prompt.

Knowing the origin of the data used can assist in the checking and interpretation of responses from the system, ensuring that responses are used appropriately.

Publicly Available Data

Data freely available via the internet, or other means that has been made generally available to the public. This information is often used to train the Foundational Model and Large Language Models of freely available AI tools, such as ChatGPT.

Providing publicly available information to an AI system is generally acceptable, noting the risks around the reliability of such information.

Any response from a freely or commercially available AI system is likely to utilise unverified publicly available information, and the interpretation of any response should acknowledge the risks associated with such information.

Tony Gee Data

Data and information created by Tony Gee through the course of operating the business or delivery of projects.

This data may be generic in nature, made available publicly, commercially sensitive or subject to copyright.

Data that can be attributed to Tony Gee should not be made available to any external AI system, as part of a prompt, or any other interaction with the system.

Every effort shall be made to anonymise data before use in an AI system.

Tony Gee data should only be used with an approved AI system (either a purchased system, or in house developed system) with appropriate safeguards in place to protect our data.

The DSG are responsible for assessing and approving the use of AI systems that utilise Tony Gee data.

Private or Copyrighted Data

We often have access to project information produced by others, information in publications, or online services we subscribe to, much of which may be protected by copyright laws.

Private or information protected by copyright, that does not belong to Tony Gee, should not be used with any AI tool.

Personally Identifiable Information

Personally identifiable information (PII) is information that, when used alone or with other relevant data, can identify an individual.

Personally Identifiable Information should not be used with any external AI tool.

Purchased and/or internally developed AI systems may be able to utilise PII with appropriate safeguards in place.

The DSG are responsible for assessing and approving the use of AI systems that utilise PII.

Use of AI Generated Content

All information created in whole or in part utilising AI tools, regardless of it's intended, and final use must be subject to review by a human with the relevant skill and expertise to validate and verify the content.

Throughout the process of creating information AI generated content should be identified, so the review can consider AI specific risks outlined in section 4.1.

Depending on where AI is used this review could be part of formal checking and approval process (i.e. information produced as part of our project deliverables, or bids and proposals) or as part of an individual's judgement in the course of their work (i.e. research, creation of internal papers or proposals).

All information we produce, including information produced with the aid of AI tools, ultimately comes from YOU, for and on behalf of Tony Gee. We must therefore be satisfied of its accuracy, reliability and it is generally fit for its intended use. All in accordance with our Quality Assurance policy, procedures and guidance.

Our clients expectations and contractual requirements should also be considered in our use of AI, for example public sector procurement in the UK now requires you to make a declaration with a tender submission if AI has been used.

Responsibilities

The DSG

Our approach to and management of AI within Tony Gee will be the responsibility of the DSG

The DSG shall ensure that this policy is reviewed regularly to ensure it remains fit for purpose.

The DSG shall maintain a register of AI systems in use within Tony Gee

All individuals

It shall be the responsibility of every individual using AI tools within Tony Gee to ensure that AI is used safely and responsibly, protecting our people and businesses.

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 Head of Digital Technology.

Compliance

Breaches of this policy may be treated as a disciplinary matter, dealt with under Tony Gee's staff disciplinary policies.

Signed:



Alasdair Fowler
Chief Executive Officer

Reviewed Date: 12 January 2026
Document No: POL-AD-003
Revision: 01

Revision History:

Rev	Date	Description
01	12/01/2026	First Issue revised format