1. INTRODUCTION

1.1 Welcome to the Six Degrees' Acceptable Usage Policy.

1.2 We are a provider of IT services, including managed cloud hosting, co-location services in our data centre, connectivity and unified communications.

1.3 In order to provide a high-quality service in compliance with the applicable legislation, this Acceptable Usage Policy apply to the use of all our services, network, equipment and systems.

1.4 This Acceptable Usage Policy explains your usage obligations, how to comply with these obligations and what will happen if your usage falls outside this Policy.

2. ACCEPTABLE USAGE

2.1 We provide communication services, IT hardware, software and network access as a resource to support your business activities. Access to these facilities is granted on the basis of this Acceptable Usage Policy.

2.2 You must conduct yourself honestly when using our facilities, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others.

2.3 You must use software and services only in accordance with the corresponding licence agreements and you must adhere to our Fair Usage Policy at all times.

2.4 We are not responsible for third-party content and material that you may access via our services.

2.5 We reserve the right to amend the terms of this Policy from time to time. We will notify you if any changes are made.

Usage Restrictions

2.6 When using our facilities, you must comply with all applicable laws.

2.7 We will not tolerate any unlawful or illegal use of our services, including:

(a) creation or transmission of information encouraging criminal skills or terrorism, human trafficking or modern slavery;

(b) download or distribution of software or data in contravention of copyright restrictions;

(c) unsolicited communications or use of personal data in contravention of any applicable data protection law, including the UK GDPR, the General Data Protection Regulation (EU) 2016/679 and the Privacy and Electronic Communications Regulations;

(d) creation or transmission of discriminatory or harassing material, pornographic or obscene content, defamatory or threatening material, or any other content which intentionally distress, offend or harm others;

(e) creation or transmission of material that might be defamatory for us or that contains adverse or derogatory comments about us or any members of our group;

(f) transmission of any data that will adversely affect, interfere with or be malicious to our or any of our third parties' network, equipment or software.

Your Responsibilities

2.8 You are solely responsible for your users' compliance with this Policy and for the use of our services.

2.9 You are responsible for all devices connected to our services and for ensuring that such devices have appropriate firewall and anti-virus software to protect you against any virus, worm, Trojan horse, or trap door program code.

2.10 You are responsible for implementing appropriate security measures to prevent unauthorised access to or misuse of our services.

2.11 You must not use our network knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of others.

3. USE OF ARTIFICIAL INTELLIGENCE (AI) TOOLS AND TECHNOLOGIES

Authorised Use

3.1 AI tools may only be used in compliance with applicable laws and regulations, including:

- UK GDPR (General Data Protection Regulation)
- EU GDPR (Regulation (EU) 2016/679)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Other applicable data protection and privacy regulations that may impact the UK.

Usage must align with this Acceptable Usage Policy, respect third-party rights, and follow ethical and legal standards.

Data Usage and Storage

3.2 Users must not upload company or customer-sensitive information into AI tools or platforms if the data's storage or processing location is unknown. If this is the case, users must seek advice before proceeding to ensure compliance with data protection laws.

Prohibited Activities

3.3 The following uses of AI tools are strictly prohibited:

- Malicious Activities: Creating or deploying malware, phishing schemes, deepfakes, or other harmful or deceptive practices.
- Privacy Violations: Conducting unauthorised data scraping, surveillance, or activities that infringe on individual privacy rights.
- Discrimination: Using AI to produce or support discriminatory outcomes based on characteristics protected under the Equality Act 2010, such as race, gender, age, religion, or disability.
- Content Misuse: Generating offensive, defamatory, misleading, or illegal content or content that promotes unethical behaviour.

Transparency and Accountability

3.4 To ensure responsible AI usage, users must maintain:

- Records: Document AI tools' purpose, scope, and operational parameters.
- Auditability: Track significant decisions made or influenced by AI, including data sources, algorithms, and outputs.
- Explainability: Ensure that AI processes are transparent to stakeholders and comply with relevant legal frameworks.

Security and Compliance

3.5 AI systems must meet high standards of security and comply with applicable laws and regulatory guidance, including recommendations from:

- UK GDPR and EU GDPR
- National Cyber Security Centre (NCSC)
- Industry best practices for securing data and preventing unauthorised access.

Breach Response

3.6 In cases of suspected misuse:

- AI tool usage may be immediately suspended or terminated.
- Incidents will be escalated to the Information Security Team for investigation.
- Where breaches involve unlawful activities, they may be reported to the Information Commissioner’s Office (ICO) or other relevant authorities.

Provider's Use of AI

3.7 Six Degrees uses AI technologies to enhance service delivery, monitoring, and optimisation. Ethical principles, industry best practices, and compliance with legal standards, including UK and EU GDPR, govern this usage. 8.8 AI Training Restrictions Users must not use sensitive, confidential, or proprietary data from the provider, clients, or third parties for AI training purposes without explicit consent.

4. HOW TO COMPLY WITH THIS POLICY

4.1 Please contact us if you require further information about this Policy, if you have any concern about your usage, or if you believe somebody has breached this Policy.

5. NON-COMPLIANCE WITH THIS POLICY

5.1 If we have reasons to believe you failed to comply with this Policy, we will attempt to contact you and give you instructions on how to remedy.

5.2 We reserve the right to disconnect or suspend your services in accordance with your Master Service Agreement if our attempts of contacting you are unsuccessful for reasons outside our control, or if you fail to comply with this Policy after being notified by us.

5.3 If a serious breach of this Policy occurs, or if we believe you have breached any laws, we may report you to and share your information with the police or any other law enforcement agency.