Enabling your brilliance

Acceptable Usage Policy

Enabling your brilliance

TABLE OF CONTENTS

1 Document Control

1.1 Issuer Details

Issuer	Six Degrees
Address	Commodity Quay, St. Katharine Docks, London, E1W 1AZ
Telephone	+44 (0)800 012 8060
Author(s)	David Miles
Reviewer(s)	SMT

1.2 Change History

Version	Date	Changes Made	Author/Editor	Approved By
1.0	23/04/2012	Initial Release		
1.1	03/12/2013	Annual review		
1.2	26/09/2014	Annual review		
2.1	16/12/2016	Annual review	David Miles	
3.0	19/12/2017	Annual review & separate from Procedure	David Miles	Daemonn Brody
4.0	14/08/2018	Upgrading to version 4.0	Kim Long	Nada Moussa Toby Clarke Toby Walsh
5.0	22/09/2019	CNS requirements added, templated updated and reviewed by CISO	Paul Rose	SMT

1.2.1 This is a CONTROLLED document. It is UNCONTROLLED when printed. You should verify that you have the most current issue.

1.2.2 Text in RED throughout to be redacted if issued outside of Six Degrees

1.3 Non-Disclosure Statement

1.3.1 This document contains intellectual property rights and copyright, which are proprietary to Six Degrees. The work and the information it contains are submitted for making a proposal, fulfilling a contract or as marketing collateral. It is to be treated as confidential and shall not be used for any other purpose. It shall not be copied or disclosed to third parties, in whole or in part, without the prior written consent of Six Degrees.

2 Introduction

2.1 Purpose

2.1.1 This policy gives guidance on the use of the Six Degrees computers and its e-mail and internet systems. This document aims to ensure that systems and IT facilities are used effectively for their intended purpose without infringing legal requirements or creating unnecessary business risks. You must accept this policy before access is granted to Company systems and you are required to adhere to its terms (which may be amended from time to time).

2.1.2 Please read this policy carefully as you will, in future, be deemed to be aware if its contents in the event that there is any breach of the Company's policy. An employee who has a question should contact the Corporate IT Department or their own line manager.

2.2 Scope

2.2.1 All staff, including employees, workers and contractors of Six Degrees, whether on a permanent or temporary basis, are subject to this policy. At the same time, individuals may be personally liable for any conduct and/or action(s) that may be unlawful or illegal.

2.2.2 Employees with access from client sites should make themselves aware of, and adhere to, any local policies for use of Internet access. Unless otherwise stated, internet access on Client's sites should not be used for non-business purposes.

2.3 Review and Development

2.3.1 This policy shall be reviewed and updated as necessary by the Six Degrees ISO and, if appropriate, by an auditor external to the Six Degrees environment in order to ensure its compliance with any changes to the law, organisational policies or contractual obligations.

2.3.2 The Six Degrees ISO by utilising both HMG and ISO27001 standards, will determine the appropriate levels of security measures applied to any new Six Degrees information systems.

3 General Principles

3.1.1 Six Degrees provides IT hardware, software and network access as a resource to support its business activities. Access to these facilities is granted on this basis.

3.1.2 This Policy is designed to help you understand our expectations for the use of those resources, and to help you use those resources wisely.

3.1.3 IT for this company is a business tool, provided to you at significant cost. That means you are expected to use your IT for business-related purposes, i.e. to communicate with clients, your colleagues and suppliers, to research relevant topics and obtain useful business information as well as to work with corporate business systems.

3.1.4 The Company insists that you conduct yourself honestly and appropriately on the internet, using email and when accessing corporate systems, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings.

3.1.5 Other Six Degrees policies also apply to your conduct using IT, especially (but not exclusively) those that deal with intellectual property rights, privacy, misuse of Six Degrees resources, sexual harassment, information and data security, confidentiality and privacy.

3.1.6 Users shall not make copies of personal information from any of Six Degrees systems other than for legitimate work-related purposes.

3.1.7 Users shall use software only in accordance with the corresponding licence agreements.

3.1.8 No Six Degrees employee will make or use unauthorised copies of any software under any circumstance. Anyone found copying software other than for back up purposes may be subject to disciplinary action. No user will give software to any outsiders, including clients, and other third parties.

3.1.9 Any user who determines that there may be misuse of software within the organisation will notify their line manager, the People team or the Corporate IT department.

3.1.10 All software used on Six Degrees owned computers will be purchased using appropriate procedures.

3.1.11 Six Degrees reserves the right to amend the terms of this policy from time to time. You will be advised of changes made.

3.2 Use of Computers and Systems at Work

3.2.1 Subject to exceptions below, the Company's computers are for business purposes only and contain information relating to the Company business. Access to the Company's network shall only be undertaken once you have been duly authorised to access and use the system and issued with a password.

3.2.2 Non-approved software exposes the Company's network to the risk of virus infection and the introduction of non-approved software may adversely affect the operation of the Company's system.

3.2.3 Any misuse of the Company's networks shall be treated very seriously and any employee who breaches the above policies shall be subject to the Company's disciplinary policy. Examples of behaviour likely to lead to action include:

- Entering the network without authority;
- Entering a part of the network to which you do not have authority;
- Using a password belonging to another employee;
- Accessing commercial or personal data when not authorised to do so or for a purpose otherwise than in connection with your duties for the Company;
- Installing and using non-approved software;
- Installing and using non-licensed software;
- Un-authorised copying and distribution of electronic copyright material;
- Un-authorised copying of personal information from any system for any activity which is not work related.

3.3 Unauthorised Access

3.3.1 Unauthorised access to another person's PC, e-mail or any part of the IT systems without due cause or authority is strictly prohibited. Tampering with, amending or deleting e-mail or other information held on Company's IT systems without authorisation or due cause is also strictly prohibited and a disciplinary offence.

3.4 Anti-Virus / Malware

3.4.1 The deliberate and reckless importation of computer virus into Six Degrees IT systems is considered a disciplinary offence and may also constitute a criminal offence committed by you under the Computer Misuse Act 1990.

3.4.2 Six Degrees uses anti-virus / anti-malware software to safeguard its systems from malicious code. All Disks, media storage devices or other transportable media (which should only be accessed if related to work purposes) must be virus checked before use on company equipment. See the Anti-Virus / Malware Policy for more details.

3.5 Passwords

3.5.1 The Password Policy details the controls that must be adhered to for the management of passwords.

3.6 Safeguarding Access to Workstations/Devices

3.6.1 You must not leave workstations/devices unattended as this could allow others to access your e-mail system and send items in your name. An automated password screensaver set to operate after 3 minutes or less of inactivity is configured to prevent unauthorised access to workstations or devices containing (or with access to) client or company information.

3.7 Hardware and Software Acquisition

3.7.1 All hardware and software required for use on the Company network must be purchased or sourced through Corporate IT. IT equipment must not be modified without authorisation from the Corporate IT. Personal software including screen savers should not be loaded onto Company IT equipment. Screensavers and system wallpapers maybe updated by Corporate IT in line with marketing initiatives.

3.7.2 All requirements for additional Hardware and software must be logged with Corporate IT.

3.8 Hardware/Software Delivery

3.8.1 All newly purchased hardware and software will be delivered to Corporate IT so that licensing can be documented, and Asset registers updated. No Hardware or Software is to be ordered and delivered direct to any other member of staff unless this has been agreed with Corporate IT in advance.

3.8.2 Any authorised local purchase or delivery must have the details, as well as documentation, licensing documentation and the original media in the case of software, forwarded to the Corporate IT for adding to the asset register.

3.9 Software Installation

3.9.1 Should you no longer require a piece of software you should log a call with the Corporate IT Service Desk to have it properly removed and the asset and licensing register updated.

3.9.2 Software that attempts to self-install when visiting web sites should always be declined and referred to the Corporate IT.

3.9.3 Shareware, Freeware and Public Domain software is bound by the same policies and procedures as all other software. If the software is to be retained the usual acquisition procedure will be followed in order to purchase a legal license to the product.

3.9.4 The use of the Company network to play Internet based games is expressly forbidden.

4 Email Use Policy

4.1 General Use of Email and Internet

4.1.1 The Company will not tolerate the misuse of the email system, business collaboration tools or the internet (whilst transmitting, retrieving, observing or storing a communication). The following types of communications may be considered misuse and may also be considered gross misconduct:

- Discriminatory or harassing in any sense whatsoever and whether prohibited by the law or not (e.g. on the grounds of sex, race, disability or age) or that could be considered offensive, obscene or in bad taste;
- Defamatory or threatening, whether legally actionable or not (e.g. in relation to other employees of the Company or the Company's competitors);
- Access to or emails relating to entertainment, sport or gambling websites or other websites which have no legitimate connection to the Company's business;
- Pornographic or derogatory to any individual or group;
- Copyrighted material without a licence to do so;
- Illegal or contrary to the Company's policies or business interests;
- Unauthorised emailing or transmission of personal information about other employees, or of confidential information about the Company, its clients or suppliers, other than for business related activities. Any such information received inadvertently should be reported to privacy@6dg.co.uk as soon as possible;
- Use of unauthorised computer software, which is software that has not been installed or approved by the Company's IT Department;
- Persistent unauthorised personal use, including but not limited to personal messages, social invitations, jokes, cartoons or chain letters.

4.2 Email/Collaboration Tools Policy

4.2.1 This section of the policy covers the use of the Company's e-mail system, and, where applicable, collaboration/communication tools (e.g. Microsoft Teams, ServiceNow LiveFeed), for internal and external communications.

4.2.2 It is important to remember that the e-mail system and collaboration tools are business systems and will be managed accordingly. E-mail can lead to the transmission of viruses, excessive network traffic using large attachments and in some cases the circulation of "unsuitable" material. All of these can prejudice the integrity and security of the Company's network.

4.2.3 Employees are required to read and follow the guidelines below.

4.3 Improper Statements

4.3.1 Be aware of what you say in messages. The apparent temporary nature of messages can result in the making of unguarded statements. However, messages are not automatically destroyed once sent and read and are often retained on the system of both the sender and the recipient. Improper statements can give rise to personal or company liability.

4.3.2 You must:

- Work on the assumption that messages may be read by others;
- Never send messages that are abusive, sexist, racist or defamatory.

4.4 Email Security

4.4.1 Incoming e-mails and their attachments may carry dangerous or potentially business damaging viruses. If you are in any doubt about incoming e-mail and the existence of a virus do not open it, you must consult the IT support staff immediately. Six Degrees utilises technical controls to manage the security of emails. Additionally these technical controls also control information classification transfer in accordance with the Information Classification and Handling Policy

4.5 Offensive or Obscene Emails

4.5.1 If you have any reason to believe that an incoming e-mail contains offensive or obscene material, you should, if possible, refrain from opening it. Under no circumstances should the e-mail be sent on to another user and it should

be deleted immediately. It should also be reported to your manager/department head. You must never download any offensive materials.

4.6 Confidentiality

4.6.1 E-mail is not a secure means of communication. Ensure any Highly Confidential, Confidential or Internal Use information sent by the Internet adheres to the requirements in the Information Classification and Handling Policy.

4.6.2 All outgoing e-mails are configured to contain your name, job title and contact information. A standard disclaimer is added to all email after your signature file so there is no need for individuals to add such disclaimers.

4.7 Presentation

4.7.1 E-mails should not be treated as an informal means of communication. You are expected to use professional language when e-mailing internally or externally.

4.7.2 E-mail is accepted in law as evidence and therefore rules regarding Data Protection and Intellectual Property apply. E-mail is "discoverable" under the process of law. The same care must therefore be taken about the content and presentation of the message as if it were a paper communication. The Company's standards of presentation for written communication, for example, the inclusion of the Company's name, number and registered office on all communications and the use of approved fonts, apply to e-mail messages. In addition, you must use the same personal and professional courtesies and considerations in e-mail messages as in other forms of communication.

4.8 Reviewing your Emails

4.8.1 E-mails should be read regularly and responded to in a timely manner. If you are going to be away for any length of time you should either:

- Arrange to access your email remotely via web mail or Company VPN;
- Set up an out of office rule to automatically forward and/or respond to mail (auto respond is not recommended if you regularly received SPAM mail as it confirms to the sender that your mailbox is active and will attract more unwanted mail). Include an alternative contact along with their contact details.

4.9 Hard Copies/Electronic Copies

4.9.1 Where appropriate, hard or electronic copies of all the e-mails which you send and receive should be placed on the appropriate file to ensure that files are kept accurate and up to date and to ensure that the complete file is preserved for the appropriate time period after archiving.

4.9.2 Users must ensure that critical information is not stored solely within the e-mail system. Hard or electronic copies must be kept or stored separately on the system. If necessary, documents must be password protected.

4.9.3 Avoid printing emails where possible.

4.10 Read Receipts

4.10.1 Consideration should be given to obtaining confirmation of receipt and/or read for important messages.

4.11 Unnecessary Messages

4.11.1 Do not create e-mail congestion by sending trivial messages or unnecessarily copying messages. Excessive use of e-mail can overload the network and waste a significant amount of your time. You are required to ensure that:

- CC should be used for contacts who you want to know about the email but are not required to action or respond to it;
- Consideration should be given before circulating emails to distribution groups (e.g. all <site>);
- E-mails are as short and accurate as possible;
- Large attachments (over 5Mb) should not be sent unless there is no other reasonably practicable way of delivering the data;
- Where possible links should be used as opposed to attachments.

5 Internet Usage Policy

5.1 Publication

5.1.1 The publication of any information relating to the Company in any way on any internet site must be approved in advance in writing by a member of the Senior Management Team.

5.2 Connections

5.2.1 Connections via Wi-Fi should be exercised with caution. Avoid connecting to unknown networks. 'Tethering' (hot spotting) should be secured. Employees are asked to note that all connections may be logged by these systems and that Internet activity may be monitored and logged and this log may be accessed if there is reasonable cause to believe that a breach of the policy has occurred.

5.3 Controls

5.3.1 As per the Internet Monitoring and Usage Policy Six Degrees operate proxy, filtering and firewall systems designed to enforce access and traffic restrictions/controls. Where present you are required to use these at all time and should not take any action that avoids the use of these controls. These systems can monitor and record all Internet usage. All users should be aware that our security systems are capable of recording (for every user) each World Wide Web site visit, each chat, news group or email message, and each file transfer into and out of our internal networks. We reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage including personal use of the Internet.

5.4 Accessing sites

5.4.1 Site access is control by technical countermeasures in the form of content control. Content permitted or prohibited is detailed in the Internet Monitoring and Usage Policy.

5.4.2 Access to non-business-related sites and personal use of the internet should only take place out of working hours.

5.5 Communication of Information

5.5.1 Each employee using the Internet facilities of the Company shall identify himself or herself honestly, accurately and completely (including the Company affiliation and function where requested) when participating in relevant social network platforms (e.g. LinkedIn) or when setting up accounts on outside computer systems.

5.5.2 Corporate mail addresses should not be used when registering on non-business-related web sites as a contact mail address.

5.5.3 Employees are reminded that social network platforms are public forums where it is inappropriate to reveal confidential Company information, client data, trade secrets, and any other material covered by existing Company secrecy policies and procedures. Employees releasing protected information via a social network platform– whether the release is inadvertent – may be subject to all penalties in accordance with existing data security policies and procedures and to disciplinary action.

5.5.4 Employees should schedule authorised communications intensive operations, such as large file transfers, video downloads, mass e-mailings and the like, for off-peak times.

5.5.5 Employees are not allowed to host, develop or administer personal Web Sites (e.g. online blogs) on company equipment.

5.6 Deliberate Misuse

5.6.1 No employee may use Six Degrees facilities knowingly to download or distribute pirated software or data.

5.6.2 No employee may use the Company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap door program code.

5.6.3 No employee may use the Company's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

5.7 Uploads and Downloads

5.7.1 Employees with internet access should not upload any software licensed to the Company or data owned or licensed by the company without explicit authorisation from the manager responsible for the software or data.

5.7.2 Any authorised file that is downloaded should be scanned for viruses before it is run or accessed.

5.8 Personal Use

5.8.1 Six Degrees does allow the limited personal use of the e-mail system, provided that such personal use does not interfere in any way with business use of the facilities, distract from your workload or jeopardise the operation of the Company's computing or electronic mail facilities, specifically bulk mailings and the joining of non-business mailing lists is prohibited.

5.8.2 Limited personal use of the Internet is also acceptable, provided such personal use does not interfere in any way with the business use of the facilities and does not jeopardise the operation of the Company's computing facilities.

5.9 Personal Privacy and Monitoring

5.9.1 The Company assumes that its staff will act in a reasonable manner and adhere to the highest standards of conduct in use of the IT Systems. The Company does monitor day-to-day email or Internet activity (via deployed technical controls). The Company reserves the right to monitor activity to ensure that the systems are being used for legitimate business purposes including the following:

- To ensure compliance with the Acceptable Use policies in force;
- To prevent or detect the unauthorised disclosure of any information which is confidential to the business of the Company (as per the Information Classification and Handling Policy). For these purposes any information held within the Company's networks is to be treated as being confidential unless the Company has taken active steps to publish the information. Confidential information includes details of the Company's client lists, suppliers, trading, margins, employees, financial or trading results, and any details relating to the Company's products and services.

5.9.2 You should note that the Company reserves the right to monitor patterns of computer use, websites accessed, connection lengths and times at which connections are made. These may be monitored for legitimate business purposes including:

- Cost analysis;
- Resource allocation;
- Optimum technical management of information resources;
- Detecting patterns of use that indicate employees are violating Company policies or engaging in unauthorised activities.

5.9.3 The Company reserves the right at its discretion to review the electronic files and messages of any user of the Company-supported Internet connection.

5.9.4 Personal e-mail messages may be open to scrutiny without your permission by network and computer operations personnel in the course of their duties. For example, by "postmasters" who may have to scrutinise e-mail which is undeliverable or otherwise problematic.

5.9.5 In accordance with the Starters, Movers and Leavers Policy when an employee leaves the Company the mailbox of the leaver remains the property of the Company. Upon leaving it is automatically presented to line manager to decide the appropriate retention period for the mailbox. The line manager will be given full access to the mailbox.

6 BYOD Acceptable Use

6.1 Purpose and Scope

6.1.1 The purpose of this section is to define acceptable use standards, procedures, and restrictions for users who have legitimate business uses for connecting a personally owned mobile device to the Six Degrees corporate infrastructure. Connecting personal devices to the Six Degrees corporate infrastructure for limited personal use is acceptable, provided such personal use does not interfere in any way with the business use of the facilities and does not jeopardise the operation of the Company's computing facilities.

6.1.2 This policy applies, but is not limited, to all devices (and accompanying media) that fit the following classifications:

- Smartphones;
- Tablet computers;
- Laptops.

6.1.3 This policy applies to any hardware and related software that is not corporately owned or supplied but could be used to access corporate resources e.g. devices employees have purchased for personal use but are also allowed to use in the business environment.

6.2 Applicability

6.2.1 This policy applies to all Six Degrees employees, contractors, third parties and other users of Six Degrees information systems who use a personally owned mobile device to access any Company or client-specific data (e.g. used for 2FA application, company email, etc.).

6.3 Affected Technology

6.3.1 Corporate IT will not directly manage personal devices, but end users are expected to adhere to the ISMS policies and procedures when connected from non-corporate equipment.

6.4 Overview

6.4.1 It is the responsibility of any person who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are applied.

6.4.2 It is imperative that any mobile device that is used to conduct Six Degrees business is utilised appropriately, responsibly, and ethically.

6.4.3 For company policies related to mobile devices see:

- Mobile Device Policy;
- Remote Access Policy.

6.5 Conditions of Use

6.5.1 All mobile devices must be protected by a password and/or biometric authentication at the welcome screen level;

6.5.2 The device should have an automatic lock which activates after no more than 5 minutes of inactivity;

6.5.3 All users must always employ reasonable physical security measures whether in active use, or in transit. This includes physical control of such devices whenever they are connected or accessing Company data.

6.5.4 Passwords and other highly confidential data as defined by the Company's Information Security policies are not to be stored or saved on mobile devices. Where this is necessary, encryption should be implemented. General work-related information should not be stored unnecessarily;

6.5.5 It is recommended that the device is protected by Mobile Device Anti-Virus/Anti-Malware software;

6.5.6 The user is responsible for installing operating system upgrades, software upgrades, and software patches;

6.5.7 All devices should have the latest recommended operating and security patches installed prior to connecting to the Six Degrees network;

6.5.8 Devices must not be jailbroken;

6.5.9 iPhone, iPad, and Apple Mac users must enable the Find My iPhone application.

6.5.10 Where appropriate MDM shall be applied on all Corporate Applications, such as Office 365

6.6 Loss or theft of Device or Data

6.6.1 If a mobile device is lost or stolen and has been used for business purposes, it is imperative that the user reports the incident to the network carrier and Corporate IT Service Desk and their line manager as soon as possible in accordance with the Incident Handling and Management Policy, .

6.7 Privacy Obligations

6.7.1 In circumstances where a device is lost, and employees use the mobile device for corporate email, Six Degrees reserves the right to wipe all data from the device (utilising the corporate MDM solution)

6.7.2 While employees have a reasonable expectation that personal information stored on their own device should remain private, the organisation's right to control corporate data and manage devices which access the corporate infrastructure may occasionally result in IT support staff unintentionally gaining access to the device owners' personal information.

6.7.3 To reduce the possibility of such disclosure, users are advised to keep their personal data separate from business data on the device, e.g. in separate directories, clearly named as "Private" or "COMPANY" and calendar appointment marked as "Private". Users are also advised to back up their personal data.

6.7.4 When employees accept the BYOD option as their business mobile device, their mobile number may be published throughout the business and as a business contact. The publication of this number is at the discretion of Six Degrees.

6.7.5 Six Degrees reserves the right to limit the ability of end users to connect to the Company network, or transfer data to it and from specific resource.

7 Enforcement

7.1.1 Any breach of this Policy by a Six Degrees user or employee will also be considered a material breach of Six Degrees Network Terms and Conditions. Six Degrees will terminate a user's right to use the Network and remove any material uploaded by that user in contravention of this Policy. If appropriate, Six Degrees will disclose information to law enforcement agencies and take any legal action against a user for breach of this Policy, including but not limited to the claim of all costs, fees, disbursements and legal fees connected therewith.

8 Glossary

Abbreviation	Description
HMG	Her Majesty's Government
BYOD	Bring Your Own Device
IA	Internal Audit
ISMS	Information Security Management System
ISO	Information Security Officer
ISOx	International Standards Organisation
MDM	Mobile Device Management

9 Definitions

9.1.1 **Defamatory material -** This is any material or information held on any medium, for example, video, picture or sound files which have the potential to injure the reputation of a person or class of persons.

9.1.2 **Obscene material -** This is material, which may deprave and corrupt persons who are likely to see it or which may be regarded as offensive. Such material is usually related to pornography, but this is not necessarily the only class of obscene material.

9.1.3 **Copyright material -** Most documents and other medium i.e. photographs, videos, music etc, are subject to copyright and as such permission may be required before transmitting or receiving copies of documents or extracts from documents.

9.1.4 **Discriminatory material -** This is any material which may be discriminatory on the grounds of race, religion, sex, disability, class or otherwise.