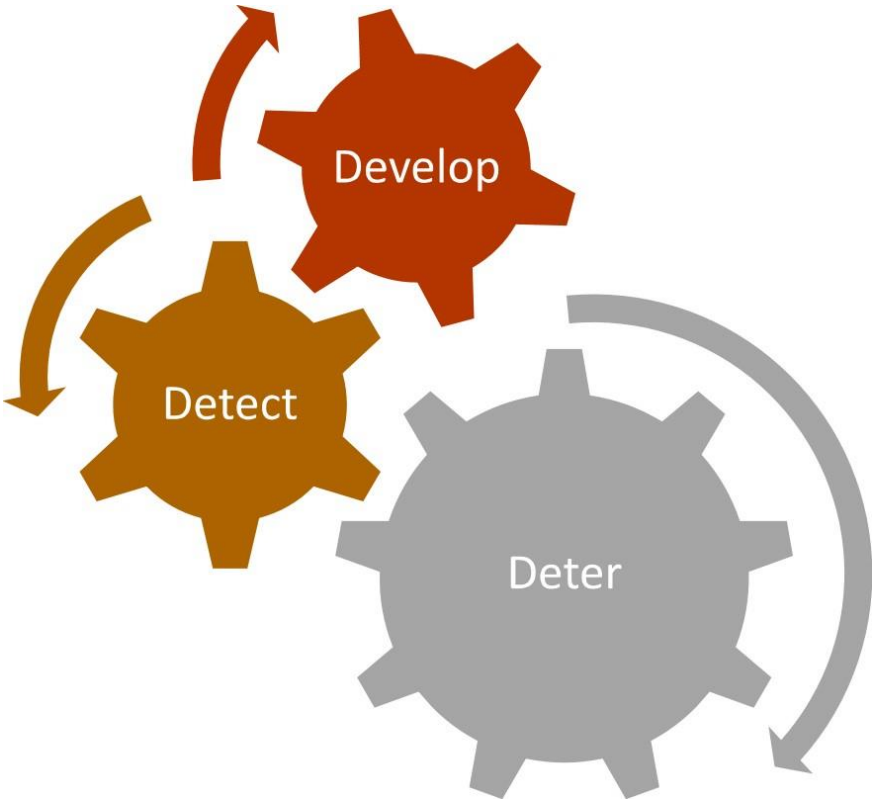
# Information Security Policies

## IS-Ola

Version 1.1



# Contents

## Information Security

Geography 4 Me is committed to the development and continual improvement of Information Security and Data Protection and its supporting Information Security Management System, in order to provide;

- Assurance with legal, regulatory and contractual obligations
- Reputation management
- Protection of critical assets
- Protection of personal data as defined by the Data Protection Act 1998 and the General Data Protection Regulations (GDPR).

Within Geography 4 Me, the terms 'Information Security' and 'Data Protection' are intended to describe the same thing, which is the pro-active protection of information/data in all its forms which is under the control of Geography 4 Me. This document can be referenced as either 'The Data Privacy Policy' or the 'Information Security Policy'.

Information is seen as a critical asset of Geography 4 Me and therefore Geography 4 Me have developed a set of policies for information security which are approved by management, published and communicated to employees and relevant external parties. These take into account;

- Business strategy;
- Regulatory, legislation and contractual needs; and
- Current and projected information security threats.

Information Security is defined as the "preservation of confidentiality, integrity and availability of information". In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved as deemed appropriate to the situation and circumstances.

The core objective of Information Security is to ensure the continuity of service of Geography 4 Me and minimise the risk of damage by preventing security incidents, managing security threats and vulnerabilities.

Information Security policies are in place to protect Geography 4 Mes informational assets against internal, external, deliberate or accidental threats and vulnerabilities.

The remainder of this document contains the policies which related specifically to Information Security. They are supported by other policies within Geography 4 Me, and are not seen as stand-alone.

# Risk Assessment & Treatment

Geography 4 Me has adopted an internal Risk control framework, which is aligned to the IS027005 standard for assessing Security Risks. A 'Risk Management Process' is documented separately, which details how risks are identified, assessed and treated.

The Risk Assessment & Treatment process includes clear lines of responsibility and delegation of authority and reporting requirements.

Risk Management is a central and essential component of Geography 4 Me's Security framework and is treated as such.

# Acceptable Use Policy

## Personal Usage of Internet & E-mail Facilities

The Internet and email facilities are an important part of the IT Systems intended to support Geography 4 Me legitimate business processes. Occasional and reasonable use of these facilities for personal purposes is regarded as acceptable provided that:

a) The IT Systems are not used for private business or other commercial purposes.

b) Use of the system does not interfere with the normal performance of your duties; and

c) There is otherwise no breach of the prohibitions identified in this or related policies.

d) The employee does not access, or use their Geography 4 Me email address to register with bulletin boards, newsgroups, comment forums or social networking sites unless authorised, or is a required part of their role.

e) Downloading and installing software or electronic media of any kind is only permitted when downloaded from a site on the safe downloads list. If you require anything not on the list please contact IT Support to ensure that it is from a reliable, legal and legitimate sources.

f) Care must be taken when emailing information that is sensitive to us, our clients or customers. The information should either be encrypted or password protected, but in all circumstances care must be taken to ensure the correct information reaches the correct recipient.

## Internet Usage

When using Geography 4 Me systems to access the Internet it must be used in a manner consistent with professional business conduct.

Geography 4 Me employs content filtering software designed to block access to inappropriate web sites or services and prevent the downloading of certain file types which are susceptible to infection by malicious software.

The Internet facilities provided must not be used for the transmitting, retrieving or storing of any communications or images that:

- Cause or may reasonably cause harassment, meaning conduct (including insults and 'jokes') which relates to gender, race, sexual orientation, religion, disability or other similar issues which are of a sensitive nature, and which cause or are likely to cause offence to any other person;

- Are defamatory - meaning the publication of material that adversely affects the reputation of a person or company;

- Are an Infringement of Copyright 'copyright' means that the owner of such material has the exclusive right to determine how that material might be copied and used. Copyrighted material must not be transmitted if the owner's permission has not been obtained; or

- Are pornographic in nature. 'Pornographic' means any material of an offensive, obscene, violent or sexual nature. There is no possible legitimate business use for accessing, transmitting or forwarding this type of material. Therefore, the question of whether or not such material constitutes pornography is not relevant to the use of the Internet, and consequently all such material is prohibited.

Use of the Internet facilities in the following manner is also prohibited:

- To deliberately propagate any malicious code such as computer viruses;
- To disable or overload any computer system or network, or to attempt to disable, defeat or circumvent any system intended to protect the privacy or security of another user; • To download or distribute pirated software or data; or
- To upload software licensed to Geography 4 Me, or to upload data owned by or under guardianship of Geography 4 Me without prior permission.

Users shall be aware that where access to web sites is permitted by filtering software, whereas that access to these web sites has not been sanctioned by Geography 4 Me, that it does not constitute acceptable sites or services. Users shall not download or save software from the internet unless specifically required as part of their job role.

Users shall not attempt to circumvent or bypass Geography 4 Me content filtering mechanisms. Should access to filtered websites be required as part of their responsibilities, users shall request access from the designated Group Technology Services Director.

## Email Usage

When provided with a Geography 4 Me email account, you must use it in a manner consistent with professional business conduct. Misuse of email can put Geography 4 Me, you and our clients at risk from breaches of confidentiality, legal liability, lost productivity and damage to reputation and services. These can lead to financial losses and/or legal penalties and would certainly impact upon our reputation.

When composing and sending an email, you must consider the consequences. In particular, you must consider whether you are likely to cause offence, enter us into any contract (intentionally or otherwise) or to commit us to any legal action. These considerations are important because emails are often drafted and sent more quickly than letters and faxes. Emails must be drafted with the same care and attention as all other correspondence. If in any doubt, you should refer to your line manager before sending the email.

Inappropriate use of email may lead to legal action against us and may lead to disciplinary action and/ or personal liability for you. In communicating with anyone via email you should not make or forward anything which could be interpreted as:

- Defamatory;
- Sexist or racist in nature;
- Derogatory, whether about an individual or a generalisation, relating to disability, religious or cultural beliefs of others; • For criminal purposes; or
- Offensive or obscene.

To ensure the safety of our clients monies, we do not store or transmit the following information;

- Payment card number (Primary Account Number or PAN)
- Card's security code (CVV2, etc.)
- Card's start and expiry dates

Geography 4 Me email accounts shall be accessed only by the owner and treated as confidential by all other employees, except where access is specifically granted for business reasons.

## Monitoring

For system performance and to ensure our systems are being used in a safe and secure manner, we may use systems and processes to monitor use of the IT Systems to ensure the effective operation of the IT Systems (e.g. virus checking, web monitoring, etc).

Our aim is to ensure that in the performance of your duties you comply with the practices and procedures which apply to us, and our own business practices and procedures, including those set out in this policy. Monitoring is also employed for the purposes of preventing or detecting crime, and for the purpose of investigating or detecting unauthorised use of our IT Systems.

Internet traffic and business emails and content may be randomly monitored. If we believe these facilities are being abused or used inappropriately, we will inform you and we will monitor traffic more specifically, which may include opening and viewing content of any business emails received or sent by you and analysis of your web-browsing activity.

Geography 4 Me routinely monitor internet and network traffic and have the right to access, review and disclose as necessary all files or messages sent or received over its networks, without regard to content but in compliance with legislative requirements including, but not limited to, the Regulation of Investigatory Powers Act 2000, the Data Protection Act 1998 and the General Data Protection Regulations (GDPR:2018).

# Access Control Policy

Access to Geography 4 Me systems is provided based upon role, and will be co-ordinated and allocated by the IT Support team. Working closely with the individual's line manager and HR, access to systems will be provided on the following basis;

- All users are assigned a unique username before being allowed access to system components or customer data.

- All users are positively identified and authenticated prior to gaining access to systems, services or data.

- Individual user's access to systems, services or information is determined in accordance with business requirements of the individual's role and responsibilities.

- Access and revoking of access to systems is managed by the IT Support team.

Access to systems will be revoked once an employee leaves the employment of Geography 4 Me using the same process which was used to provide access.

# Clear Desk Policy

Confidential or sensitive information, whether held electronically or on paper records and other valuable resources must be secured appropriately when you are absent from your workplace and at the end of each working day.

To facilitate this, the following guiding principles have been produced which cover both non-electronic (e.g. manual/paper files) as well as electronic forms of information.

- Desks must be cleared at the end of each working day of any confidential or personal identifiable information. Files containing confidential information must be locked securely in desks, filing cabinets or designated secure rooms at all times, other than when being used by staff. Every effort must be made to keep this information secure and not readily accessible to non-authorised staff.

- To reduce the risk of a breach of confidentiality and adherence to the Data Protection Act (DPA) and GDPR, when disposing of personal identifiable information, ensure that it is destroyed securely using approved methods of waste disposal (i.e. shredding).

- Personal items (i.e. keys, handbags, wallets etc.) should be stored safely in the interests of security. It is the responsibility of the owner to ensure all security precautions are taken.

- Health & Safety — desks and other work spaces should be sufficiently tidy at the end of each working day to permit the Geography 4 Me' cleaning staff to perform their duties.

- When staff are working from home, or other non-office based locations, it is important that they continue to adhere to the principles of this policy and raise any concerns with the Data Protection Manager immediately.

# Mobile Device & 'BYOD' Policy

Mobile devices are provided to individuals who require them as part of their role, but before doing so, they are configured with appropriate password controls. The technology used automatically encrypts the data stored upon them in line with industry standard levels of encryption. Employees may use their own mobile telephone devices ('Bring Your Own Device' — BYOD), in line with the Employee Handbook, but need to agree to the security controls being enforced on that device to do so.

# Supplier Security Policy

All third parties with access to data or information provided by Geography 4 Me, have a current and up to date Non-Disclosure Agreement (NDA) or contract in place, which sets out clear guidance on the service provided. Suppliers information is held centrally, within Geography 4 Me, and the suppliers are subject to periodic audits and reviews by the organisation. A detailed procedure is available, which identifies the requirements of this policy.

# Passwords

Passwords are an important element of Information Security, and care must be taken when creating, using and changing them. All users of Geography 4 Me systems must have a unique User ID, and shall require authentication by password and 'two-factor authentication' (e.g. something you 'have' and something you 'know').

Passwords are for individual users in order to maintain accountability, and must be different from User IDs. Passwords should be kept confidential, and must not be written down or saved within the information system unless within an approved password safe (or Vault).

All passwords used within Geography 4 Me have the following characteristics:

- Minimum length and format.
- A maximum validity period.
- Password re-use limitation.
- Number of unsuccessful login attempts allowed.

There is a process in place for the revoking and resetting of passwords, which is described more fully in the "IT Password Policy".

# Data Protection Policy

Geography 4 Me is classed as a Data Controller in some circumstances and Data Processor in other under the current Data Protection Act 1998, however Geography 4 Me recognises that under the new General Data Protection Regulations (GDPR:2018) our obligations to ensure appropriate controls are in place, irrespective of classification, is of critical importance.

We are committed to protect the privacy of data subjects, who include our customers, clients, employees and other interested parties. Geography 4 Me have engaged in a programme of Information Security Management which is aligned to the international standard, IS027001 :2013 to ensure that the processing of personal information is conducted using best practice processes.

The following sections, detail Geography 4 Me practices which are directly linked to Data Protection requirements, and are supported by further policies and procedures which can be requested by data subjects.

## Transmitting Personal Data

Where personal data is to be transmitted (either electronically or in hard copy), staff are required to ensure that any such data is secured using appropriate measures (e.g. Use of encryption, passwords for electronic transmissions or using secure couriers).

Personal data will only be transmitted in accordance with Geography 4 Me pre-agreed processes and with best practice in-mind.

Personal data is only transmitted to a person authorised to receive it in compliance with these Data Protection principles.

## Storing Personal Data

Personal data in hard copies (e.g. paper medical records, copy passport etc) are retained only for as long as is essential to the account and/or customer, employee or other interested party that they refer to.

Personal data in hard copies or electronic formats will be stored in accordance with best practice which are part of a broader Information Security Management System (ISMS) which is aligned to the international standard for Information Security, IS027001 :2013.

The management of personal data is controlled through this standard and Geography 4 Me have committed to ongoing audit and review of policies, processes and practices associated to holding information in all its form.

## Incident Management & Data Breaches

Geography 4 Me understands there is no greater responsibility than the protection of the data held in relation to our people, clients, and our workplaces, and therefore we have ensured that appropriate controls are in place to reduce the likelihood of an incident occurring. However, in the unlikely event of an incident occurring, Geography 4 Me have established a process to reduce the impact upon our staff, clients, and our business. These processes include the management of 'Data Breach .

If any breach of the DPA, GDPR or its principles occurs, staff are required to inform the Data Protection Manager to be logged and investigated, in line with the "Geography 4 Me Data Breach Policy".

Upon notification and initial investigation Geography 4 Me will ensure that, where deemed necessary, both the Information Commissioners Office and the data subjects affected will be informed without undue delay.

## Subject Access Request (SAR)

An individual has the right to see what personal information is being held about them by Geography 4 Me. If an individual makes a written request to us and asks for information under the Subject Access Request provisions, they are entitled to request:

- information on whether any personal data is being processed; • what personal information is being held by Geography 4 Me;

- a description of the personal data, the reason it is being processed and whether it is shared with third-parties (and know who they are); • details of the source of the data

Where any Subject Access Request is received, Geography 4 Me will not charge for such a request and will work with the individual making the request to understand what is the nature of the request and provide this information within one month of the request being made.

## Responsibilities

Geography 4 Me recognises it has a responsibility to ensure that personal data is protected using appropriate technical and operational measures and as such has implemented a security framework which focuses on both operational and technical aspects of Data Protection. In this regard Geography 4 Me have;

- Implemented controls to ensure that staff cannot gain access to information that is not necessary for them to carry out their job functions.
- Put in place measures to ensure that all information held will be relevant, accurate and upto-date and used only for the purpose for which it is required and was originally intended.
- Committed to ensure information will not be kept for longer than is necessary and will be kept secure at all times.

Geography 4 Me staff who manage and process personal or sensitive personal information will ensure that it is kept secure and sensitive personal information will only be processed fairly and lawfully, and in line with the provisions set out in the relevant Data Protection regulations.

Geography 4 Me ensure that all staff are made aware of the reasons why personal and sensitive personal data is being processed and are provided with frequent and ongoing training and support with regards to Data Protection.

## Data Classification

Geography 4 Me is committed to the protection of information held or processed on corporate systems, or systems belonging to third parties. In particular, Geography 4 Me are concerned with information which is classified as 'Confidential' (as per this policy).

In order to correctly understand where confidential information exists within Geography 4 Me, and to what degree that information requires protecting, the company has undertaken a review of the data it holds, as part of a broader 'General Data Protection Regulation' (GDPR) programme. However, it is important to state that information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

Classifications and associated protective controls of information take account of business needs for sharing or restricting information, as well as legal requirements. Owners of information assets are accountable for their classification.

## Labelling of information

Information held by Geography 4 Me is assigned a 'label' based upon their Classification. This labeling of information within Geography 4 Me follows a standard information classification scheme adopted by many organisations;

- Confidential - Highly sensitive or valuable information (e.g. Client/personal data) must not be disclosed outside of Geography 4 Me without first ensuring appropriate safeguards are in place and the sharing of such information is necessary to fulfil a business purpose.

- Internal Protected - The default assumption is that all data is Internal Protected unless specifically identified as Confidential or Public.

- Public — Information that may be broadly distributed without causing damage to Geography 4 Me its employees and stakeholders (e.g. marketing materials). These documents may be disclosed or passed to persons outside the organisation.

Documentation created within Geography 4 Me, should carry one of the above 'labels' in the header of footer of the document (e.g. see this document) Where no marking is shown on information within Geography 4 Me it is always deemed to be Confidential and should be treated as per above

### Data Retention & Destruction

Information shall only be held for as long as necessary to carry out the legal obligations of the contract in place between Geography 4 Me and our clients, and in line with UK legislation. Retention of data is based on the needs, expectations and rights of the UK and European citizens. There is a full 'Data Retention Policy' in place which outlines what these retention periods are.

When destroying data, all reasonable steps to ensure the information is destroyed in a suitable manner must be taken, to ensure the confidentiality is maintained. This includes physical documentation, electronic media and information held electronically. Care and thought must be taken to ensure that the disposal of information does not expose our customers, clients, employees or Geography 4 Me to data risks.

Measures include the use of paper-shredders, and destruction of hardware is handled by our IT Support team.

## Cryptographic Key Management

Geography 4 Me recognise the important role that encryption has to play in ensuring information security, however due to the processes involved within our business we feel that the use of encryption is not required. Therefore, we do not utilise encryption tools, which require specialised 'keys'. This stance is continually in review and should this situation alter, this policy will be amended appropriately.

## These Policies

This document, and the policies within it are subject to ongoing review as part of the annual review cycle and are signed off, annually by the CEO of Geography 4 Me, who is ultimately accountable for Information Security at Geography 4 Me.

# Enforcement

By utilising the IT Systems provided and undergoing appropriate training, each employee, contractor and consultant are bound by this policy from the beginning of their employment or contract (as the case may be). You may also be prompted to accept or re-accept its conditions when attempting to access the IT Systems, which may from time to time include revisions to this policy. If so prompted, you should ensure that you carefully read any such policy. By continuing to use the IT Systems, you will be deemed to have accepted, and shall comply with any such revised policy.

In addition;

a) You are bound by this policy, and breaches of it may be treated as misconduct/ gross misconduct, and be dealt with within the framework of Geography 4 Me disciplinary procedures.

b) The level of misconduct will be dependent upon the severity or persistence of the breach. For the avoidance of doubt, any activities which are identified in this policy as "prohibited", may be treated as misconduct or gross misconduct. If you have a grievance associated with the use of the Internet or email, you should refer to the Geography 4 Me grievance policy for guidance.

c) After termination of your employment or contract you remain contractually bound not to disclose or make use of confidential information or trade secrets which could result in Geography 4 Me being damaged commercially or in reputation as per the appropriate clauses in your employment contract.

d) Failure to adequately comply with this policy and other documents referred to in it may lead to disciplinary action.

e) Geography 4 Me reserves the right to take legal action against any ex-employee who breaches the content of point d) above.

If you have any questions about this policy or do not understand any part of it, you should contact your line manager as soon as possible.